ValiCert® Enterprise VA™

Installation and Administration Guide

Version 3.2

ValiCert®

Securing e-Transactions™

ValiCert, Inc.
1215 Terra Bella Avenue
Mountain View, CA 94043

Part Number: DCU-B-ESAG-0320E

Revision: 0215-0

Table of Contents

Preface

1 Introduction

2 Getting Started

B Security Recommendations

C Security for VA Administration

D Setting up Hardware Acceleration Feature

E Using the SNMP Agent

F Troubleshooting

Index

Preface

About This Guide

This manual describes the installation, configuration, and administration, of the ValiCert Enterprise Validation Authority (VA).

Audience

This guide is intended for ValiCert Enterprise VA server administrators and corporate security analysts.

The server administrator is defined as a system administrator, or network administrator, who is responsible for installing, configuring, and maintaining the ValiCert Enterprise VA.

The ValiCert Administrator is any of the following:

- Customers with technical networking background and experience.
- System administrators who are familiar with the fundamentals of digital certificates and validation.
- System administrators who are responsible for installing and configuring software packages.

Organization of This Guide

This guide is organized in the order that a server administrator would encounter events during installation, configuration, and operation of the security software.

Section	Description
Introduction	Provides an overview of the Enterprise VA and its features.
Getting Started	Describes how to install your ValiCert Enterprise VA.
Setting Up Enterprise VA	Explains how to configure the Enterprise VA at the Setup menu of the web-based ValiCert Administration Server graphical user interface
Working at the Configuration Mode Menu	Describes the various management and configuration tasks that you can perform at the Enterprise VA Management menu
Writing a VA Extension	Provides information to help you write an extension that extends the functionality of the Enterprise VA to include Stateful Validation™ that is, application-specific or context-specific processing tailored to your requirements.
Using the Directory Update Extension	Describes the ValiCert Directory Update extension which is provided as part of the Enterprise VA package and how to use it.
VA API Reference	Provides reference information about data structures, functions, error codes, and notification types available to developers who are implementing a VA extension.
Using Delegated Certificates	Provides procedures for issuing delegated certificates.
Security Recommendations	Provides security measures that can be taken to prevent unauthorized access to the Enterprise VA.
Security for VA Administration	Provides instructions for setting up a secure session on Windows NT and UNIX.
Setting up Hardware Acceleration Feature	Provides troubleshooting information.

Typographical Conventions

The following typographical conventions are used in this guide to help you locate and identify information:

Italic text is used for emphasis and book titles.

Bold text identifies menu names, menu options, items you can click on the screen, and keyboard keys.

`Courier font` identifies commands you enter at the command line, file names, folder names, code, and text that either appears on the screen or that you are required to type in.

The base directory that houses all of the components of Enterprise VA is referred to as `<VAInstallDir>`. The actual location depends on where you install Enterprise VA.

NOTE: Notes provide significant, helpful information about a feature, operation, or procedure.

Abbreviations and Acronyms

The following list is provided of terms used in this manual, and in the internet security field:

Abbreviation/ Acronym	Definition
CA	Certificate Authority, entity that issues certificates
CRL	Certificate Revocation List, list of revoked certificates
CRLDP	CRL distribution points, geographically or functionally localized CRLs
CRT	certificate revocation tree
DN	Distinguished Name, a unique naming scheme
LDAP	Lightweight Directory Access Protocol

Abbreviation/ Acronym	Definition
MIME	Multipurpose Internet Mail Extensions
MOSS	MIME object security service
OCSP	Online Certificate Status Protocol
PKCS	Public Key Crypto Standards
PKI	Public Key Infrastructure
S/MIME	Secure MIME
SHA-1	Secure Hash Algorithm
SSL	Secure Socket Layer
VA	Validation Authority
x.509	international standard for digital electronic documents

ValiCert Documentation

- ValiCert Enterprise VA™ Installation and Administration Guide
- ValiCert VA Publisher™ Installation and Administration Guide
- ValiCert Validator Suite™ Installation and Configuration Guide
- ValiCert Validator Toolkit™ Programmer's Guide

Technical Support

ValiCert provides debugging assistance, integration assistance and general customer support. Please contact us through one of the following methods:

- Email: support@valicert.com
- Telephone: +1.650.567.5469
- Fax: +1.650.254.2148

When you contact us, we would appreciate your sending us as much detailed information as possible regarding your:

- Network
- Platform

- Specific problem and how to reproduce it.

Credits

This product contains encryption software from RSA Data Security, Inc. Copyright © 1994 RSA Data Security, Inc. All Rights Reserved.

This product includes portions of SSLeay software written by Eric Young (eay@mincom.oz.au). Copyright (C) 1995-1997 Eric Young. All rights reserved. This product includes software written by Tim Hudson (tjh@mincom.oz.au).

This product includes software from Netscape Communications Corp. Copyright (C) 1997 Netscape Communications Corp. All rights reserved.

This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/).

CHAPTER 1

Introduction

The ValiCert® Enterprise Validation Authority™ (Enterprise VA) is the flagship component of ValiCert's complete validation solution which provides your organization with increased trust and security before engaging in secure communications and electronic commerce over the internet. The ValiCert solution provides CA interoperability, scalability to support a growing number of digital certificates, simple "policy management" administration, and high-performance validation.

The Enterprise VA provides high-performance certificate validation for a corporate intranet. It requests and receives revocation lists from the network's certification authority (CA) or certificate server.

NOTE: The Enterprise VA is CA neutral. This means that the Enterprise VA can receive validation requests from any applications and from any Certificate Authorities (CAs) issuing certificates.

The Enterprise VA provides validity status responses for any X.509 certificate, and can use any of today's most widely used certification status checking mechanisms. The Enterprise VA supports the following mechanisms:

- ❖ Certificate Revocation Lists (CRLs)
- ❖ CRL Distribution Points (CRLDPs)
- ❖ Online Certificate Status Protocol (OCSP)

In addition, ValiCert provides it own proprietary mechanism called Certificate Revocation Trees (CRTs). CRT is a high-performance technology used to format the revocation information and make it available to client applications that have received certificates and need to validate them.

Product Architecture

The extensible architecture of the ValiCert Enterprise VA (and ValiCert Validation Toolkit) opens up opportunities for innovative third-party development. ValiCert's open systems approach, interconnected by standard-based protocols and open API, gives developers the flexibility to develop extensions that are appropriate for their specific needs. For example, a third-party developer could write an extension to support policy decisions that apply to any of a number of information repositories such as a credit information source, human resource data, bank data, or some other custom information source.

The Enterprise VA is comprised of three primary components:

- Enterprise VA Host
- Enterprise VA Administration Server
- VA API

Figure 1 provides an overview of the Enterprise VA components and their relationship to one another and components that use the Enterprise VA.

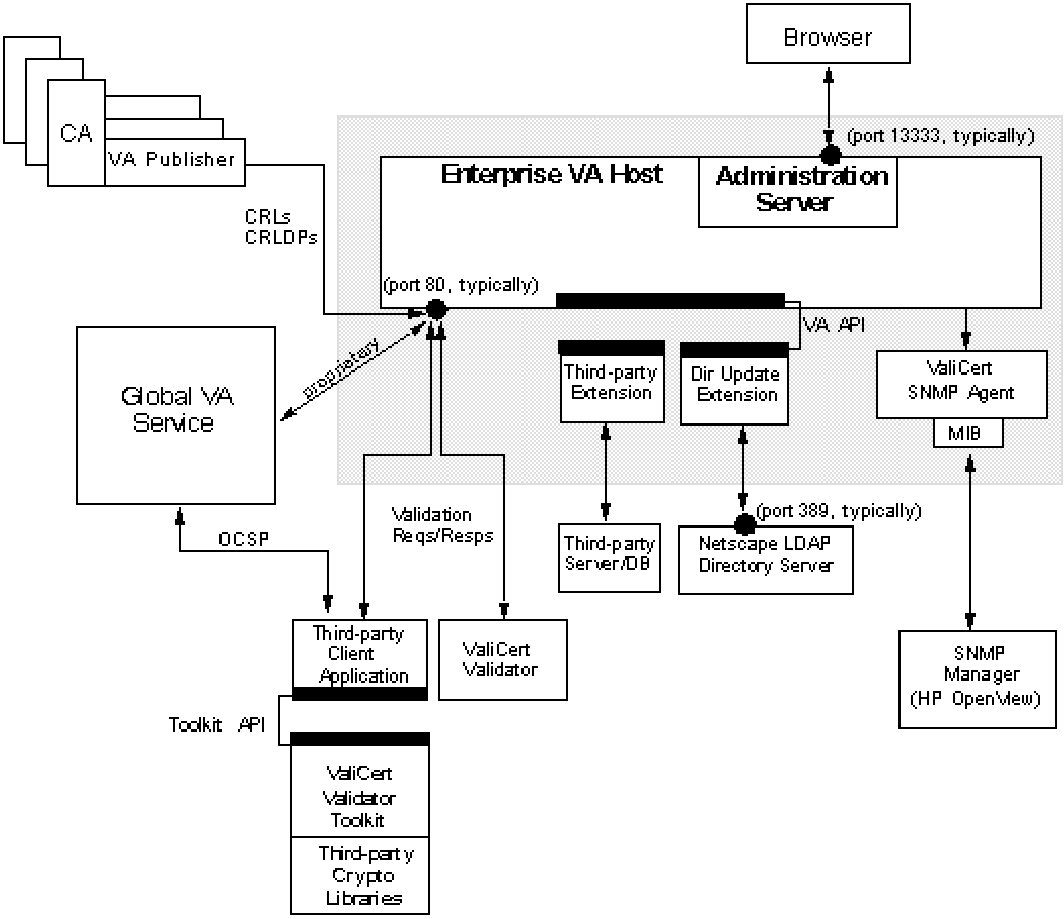


Figure 1. Enterprise VA Component Overview

Enterprise VA Host

The Enterprise VA Host is the validation engine of the Enterprise VA. All validation processing done by the Enterprise VA is done by the host. It can run in a Windows NT or UNIX environment.

Enterprise VA Administration Server

The Administration Server provides web-based installation and management of the ValiCert product components as well as any extension that may be included. The Administration Server can provide centralized management and configuration of your organization’s validation processing. It can run in a Windows NT or UNIX environment.

VA API

ValiCert supports extensions to the Enterprise VA to expand validation to include Stateful Validation™ that is, application-specific or context-specific validation processing. The Enterprise VA provides an open API called the VA API. The VA API gives customers the flexibility to further extend the Enterprise VA to include Stateful Validation tailored to their own requirements. This means your organization can integrate your specialized validation needs into the validation processing already provided by the Enterprise VA. For more information about how this can be done, see Chapter 5, "Writing a VA Extension."

NOTE: Your validation extension integrates into the validation request processing of the Enterprise VA.

Currently, the Enterprise VA includes the Directory Update extension, which provides full directory integration with the Netscape Directory Server and the flexibility to work with any LDAP directory. For more information, about the Directory Update extension, see Chapter 6, "Using the Directory Update Extension."

SNMP Support

Enterprise VA supports the Simple Network Management Protocol (SNMP) and provides an SNMP agent to help you monitor the Enterprise VA through an SNMP Manager such as Hewlett Packard OpenView or Trivoli.

The following figure shows the relationship between the Enterprise VA, ValiCert SNMP Agent, and SNMP Manager.

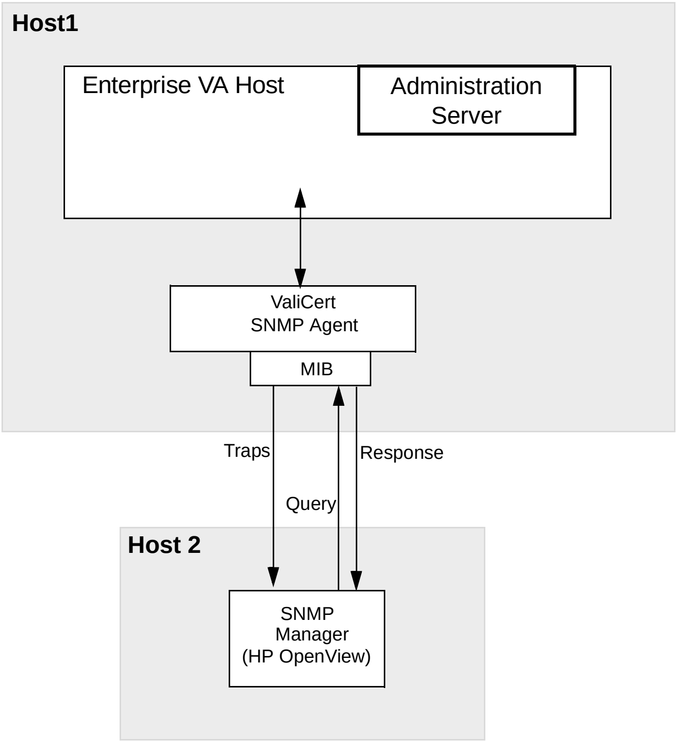


Figure 2. SNMP Support Overview

The ValiCert SNMP agent runs as a process separate from the VA Host and Administration Server processes. However, it must run on the same host. It acts on their behalf to provide updated MIB variables that can be monitored by the SNMP Manager.

The supported MIB variables describe the following:

- Status and error information
- Traps

The SNMP Agent updates the MIB variables periodically. The SNMP Manager sends a query to the SNMP agent, that is, it performs a GET or GETNEXT SNMP operation to read the current values of the MIB variables. The MIB variables are maintained in the ValiCert MIB. The Manager displays this information at its user interface.

A trap is a message that is triggered by an event, for example if the server is down. If the SNMP Agent discovers that one of the trap-triggering events has occurred, it updates the corresponding MIB variable and sends a trap message to the SNMP Manager. Once the SNMP Manager receives a trap message it can alert the user. How the user is alerted is configurable.

The type of information that is tracked by the SNMP Agent and can be monitored at the SNMP Manager is as follows:

- Service/daemon health
- Service/daemon state information
- Service error/warning information
- Service/daemon Up/Down status

For details about the MIB variables and the corresponding information available through the SNMP Manager, see Appendix E, "Using the SNMP Agent."

Hardware Signing

Enterprise VA supports version 2.1 of RSA security’s PKCS #11 specification. The specification allows for hardware signing and acceleration using hardware modules with specific interoperability with Chrysalis and nCipher modules.

CHAPTER
2

Getting Started

This section describes how to install ValiCert Enterprise VA. Use the setup program to install the ValiCert Enterprise VA from the CD-ROM. Use the product's administrative web server to configure the Enterprise VA, manage certificates, and start and stop the server.

To install the Enterprise VA, install the following components:

- ❖ Enterprise VA Administration Server
- ❖ Enterprise VA Host Server
- ❖ Netscape Directory Server extension (optional)

Before you Begin

Before you begin the installation process, be sure that the following requirements are met:

- ❖ System Requirements
- ❖ Pre-installation Tasks

System Requirements

Be sure that your system meets the system requirements listed in Table 1 for Windows NT systems or Table 2 for UNIX systems.

Table 1 lists the system requirements for installing the Enterprise VA on Windows NT.

Table 1. System Requirements for Windows NT

Requirement	Minimum	Recommended
Hardware	Intel Pentium-based or compatible systems	Intel Pentium-II based or compatible systems
Memory	32 MB	64 MB
Disk Space	100 MB	100 MB
Operating Systems	Windows NT Workstation 4.0 or Windows NT Server 4.0 *	Not applicable

* Use Service Pack 5 or later.

Table 2. System Requirements for UNIX

Requirement	Minimum	Recommended
Hardware	Sun SPARC-based workstation	SunUltra or compatible
Memory	32 MB	64 MB
Disk Space	100 MB	100 MB
Operating Systems	Solaris 2.5.1/2.6/2.7	Not applicable

Pre-installation Tasks

Before you install any software, perform the following pre-installation tasks:

- Be sure you have administrative privileges on the machine where you will be installing the Enterprise VA Administration server.
- We suggest that you make port 80 available to the ValiCert Enterprise VA for accepting validation requests. Typically, this means that you cannot have a public web server running on the machine because most web servers run on port 80 by default. You may assign the ValiCert Enterprise VA a port number other than 80; however, you will also need to reflect this change in the ValiCert VA Publisher and any ValiCert Validator Suite components that you have already installed or plan to install.
- For a local setup, be sure that you have a CA that is up and running. You will need access to this server over the network to install its certificate in

the ValiCert Enterprise VA’s certificate store. The ValiCert Enterprise VA uses the certificate to check the validity of the certificate revocation list (CRL) data that it receives from the VA Publisher installed on that CA.

- Be sure that your certification authority (CA) and client application(s) are able to communicate certificate information with each other.
- Be sure that the machine on which you plan to install the Enterprise VA has Netscape Communicator 4.7 or later or Microsoft Internet Explorer 5.01 or later.
- If you have encryption hardware connected to your server to generate the key pair make sure you have the correct version. See Appendix D, "Setting up Hardware Acceleration Feature."
- Determine whether this is a new installation or an upgrade. If this is an upgrade, you need perform the tasks described in “Upgrading to Enterprise VA 3.2” on page 9 before you install.
- Determine whether you will be using a self-signed certificate or a delegated certificate. For information about issuing delegated certificates, see Appendix A, "Using Delegated Certificates."
- Review the security recommendations listed in Appendix B, "Security Recommendations."

To install on Windows NT, proceed to “Upgrading from Certificate VA 3.x on NT” on page 21.

To install on UNIX, proceed to “Installing Enterprise VA on UNIX” on page 30.

Upgrading to Enterprise VA 3.2

The procedure for upgrading your Enterprise VA depends on the current version and platform. For versions 2.x and lower on all platforms you must manually remove the old version and then install the new version.

For versions 3.x and higher, the NT installer performs an automatic upgrade. For versions 3.x and higher on UNIX you must manually preform the upgrade.

If you have any custom extensions installed in your Enterprise VA, before you upgrade follow the steps in the "Upgrading Custom Extensions" below.

To upgrade your Enterprise VA to version 3.2. follow the procedures described in one of the following sections:

- Upgrading from Enterprise VA 3.x on NT

- ❖ Upgrading to Enterprise VA 3.2 on UNIX
- ❖ Upgrading from Certificate VA 3.x on UNIX
- ❖ Upgrading from Certificate VA 3.x on NT

Upgrading Custom Extensions

If you have any custom extensions installed, follow these procedure for each custom extension:

The

NOTE: The system extensions are upgraded automatically. Preform these steps for custom extensions only.

Step 1 Make a back up of the .dll file (for Windows NT) or .so file (for UNIX) and the .ecf file for each extension.

Step 2 Upgrade your Enterprise VA, following the directions in the appropriate upgrading section. When you upgrade the Enterprise VA, a backup copy of the `entserv` directory (including `vcconfig.ini`) is created.

Step 3 For each extension, add the following line to the `valicert.ini` file:

```
EVAExtensions = <extension_file_path>
```

Where `<extension_file_path>` is the path to the .dll or .so file. This path can be relative to the `entserv` directory. The order the extensions are listed determines the order in which extension processing occurs if more than one extension is requested at the same stage.

Step 4 Copy the .ecf file for each custom extension into the `entserv` directory.

Step 5 In the `vcconfig.ini` file:

For each custom extension, increase the value of `NO_OF_EXTENSIONS` by one. For example if `NO_OF_EXTENSIONS = 2` and you are adding 2 custom extensions set `NO_OF_EXTENSIONS = 4`.

Step 6 For each custom extension, copy the `EXTENSION_n` section from the old `vcconfig.ini` file into the new `vcconfig.ini` file. Copy the following three variables:

```
[EXTENSION_n]
NAME=Your Custom Extension
INPUT_INI=CustomExtensions.ecf
```

Step 7 Re-start the Enterprise VA for the changes to take effect.

Upgrading from Enterprise VA 3.x on NT

To upgrade from a version of Enterprise VA that is 3.0 or higher (3.x) run the installer. The installer detects the previous version.

NOTE: Stop the Enterprise VA server and the Apache (administration) server before you upgrade.

To upgrade the ValiCert Enterprise VA on Windows NT

Step 1 To start the installer, click on Setup.exe.

A dialog displays asking if you want to upgrade.

Step 2 Click **Yes** to upgrade.

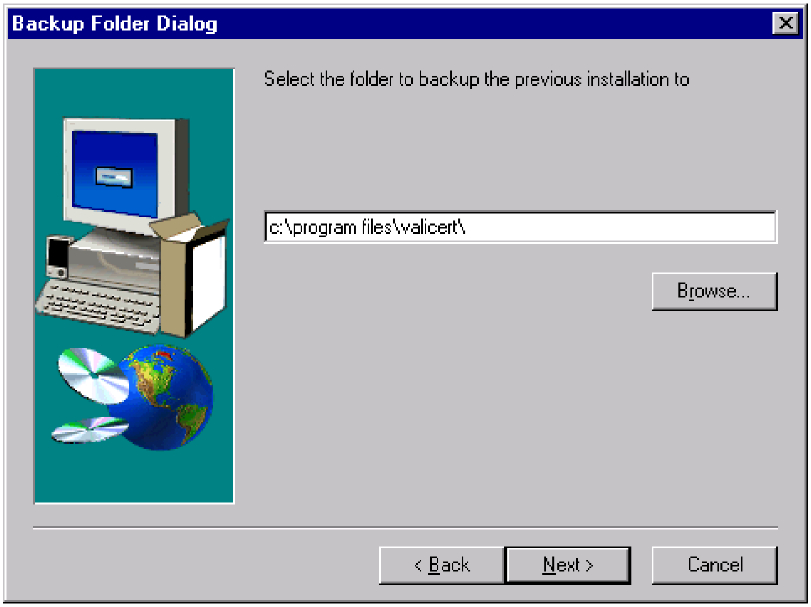
The Welcome dialog displays.

Step 3 Click **Next**

The Software License Agreement displays.

Step 4 Click **Yes** to accept the terms of the agreement.

The Backup Folder dialog displays.



Select the folder to backup the previous installation to

c:\program files\valicert\

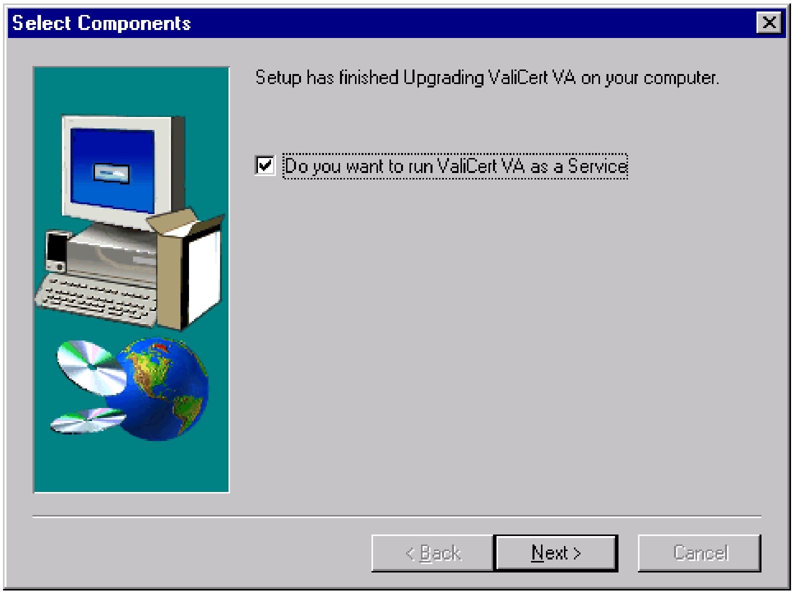
Accept the default location or select a location to backup the current installation.

Step 5 Click **Next**.

A backup of the `<InstallVadir>` directory is made.

Step 6 Click **OK**.

The software installs and the following dialog displays.



Select Components

Setup has finished Upgrading ValiCert VA on your computer.

☑ Do you want to run ValiCert VA as a Service

Select if you want to run the Enterprise VA as a service.

Step 7 A password dialog box displays.

Step 8 Enter the password for the previous Enterprise VA installation.

Step 9 Click **OK**.

The Setup Complete dialog box displays.

To read the latest ValiCert Enterprise VA information now, select **Yes, I want to view the Readme File**.

To start the Enterprise VA Administration Server now, select **Yes, I want to launch Admin Console**.

Step 10 Click **Finish**.

Upgrading to Enterprise VA 3.2 on UNIX

To upgrade to Enterprise VA 3.2 on UNIX, you must back up certain files, manually remove the application, install the new application and then copy the appropriate files and variables to the new installation.

The following flowchart diagrams the steps for upgrading you Enterprise VA on UNIX.

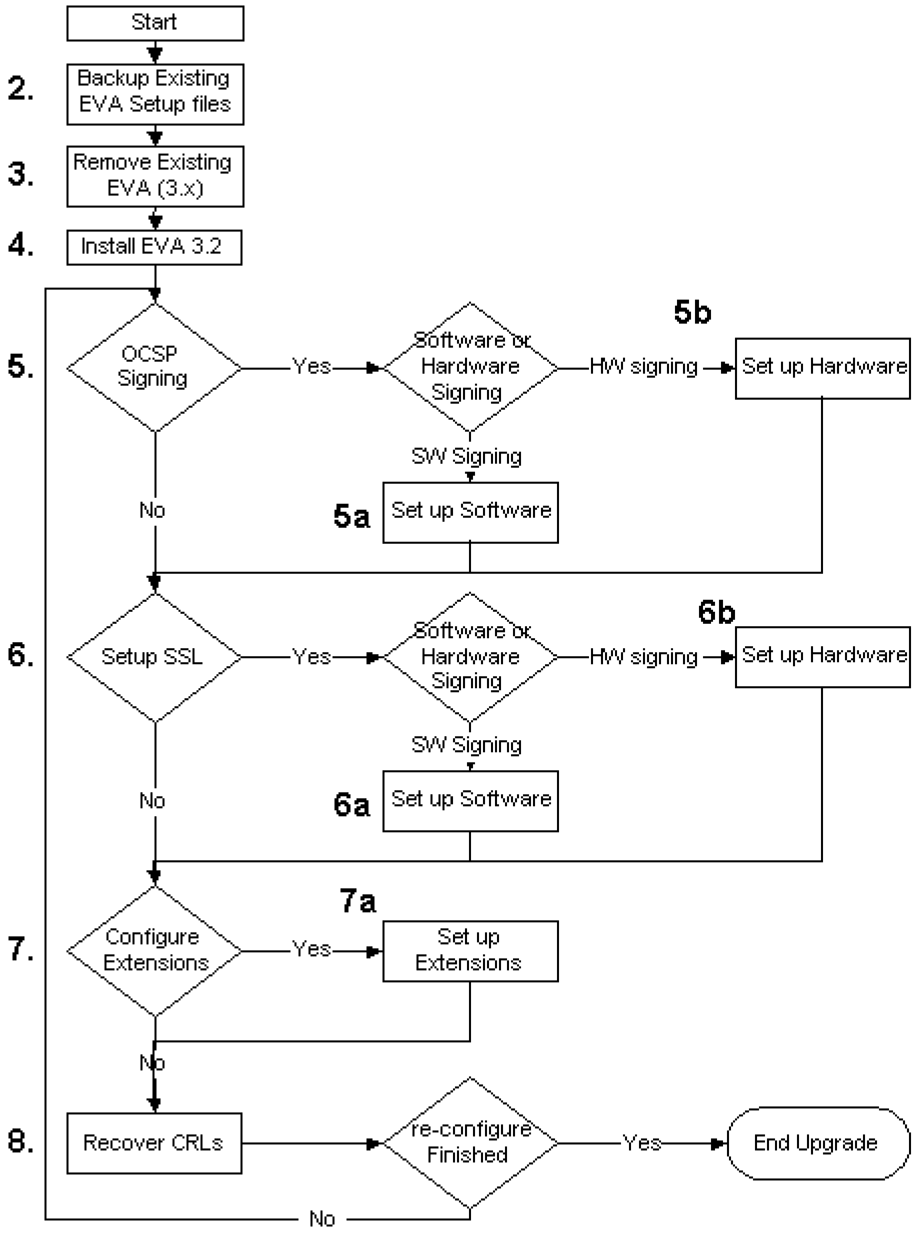


Figure 3. UNIX upgrade steps flowchart

The following instructions are for using your existing configurations with Enterprise VA 3.2. All of the settings can be configured through the Administration web pages.

NOTE: Some file names specified in the two `valicert.ini` files differ. Make appropriate changes in the new `valicert.ini` file so that the variable values are consistent with the files specified in the old file.

In addition some of the file names are configurable and may be different from the ones shown in this example.

To upgrade to ValiCert Enterprise VA on UNIX

Step 1 If necessary stop the Enterprise VA and the Enterprise VA Administration Server.

Step 2 Backup the `entserv` directory.

You will use the files in this directory in your Enterprise VA 3.2 installation.

NOTE: After copying any files from the backed up directories make sure to change the user and group to `nobody`. All the files in `entserv` directory are owned by `nobody:nobody`.

In Enterprise VA 3.2, all subdirectories are created under the directory named `va` as opposed to `enterpriseva` in Enterprise VA 3.01.

Step 3 Uninstall Enterprise VA 3.01 and clean the directory.

Remove the Enterprise VA Administration Server and the Enterprise VA.

Step 4 Install Enterprise VA 3.2.

Refer to the “Installing Enterprise VA on UNIX” on page 30 for detailed information about installing the Enterprise VA.

Step 5 The method to configure OCSP signing depends on whether you are using hardware or software signing.

a) For Software Signing, copy the following files from the backed up `entserv` directory to the new `entserv` directory:

`license.dat`

`ca.cert` (or the file pointed to by the `certFile` variable in the old `valicert.ini`)

If present, `default.cert` (or the file pointed to by `defaultSelfCertFile` variable in the old `valicert.ini`)

If present, `cacrl.cert` (or the file pointed to by the `selfCertFile` variable in the old `valicert.ini`)

`cacrl.privkey` (or the file pointed to by the `privKeyFile` variable in the old `valicert.ini`)

`cacrl.req`

b) For Hardware Signing, copy the following files from the backed up `entserv` directory to the new `entserv` directory:

`license.dat`

`ca.cert` (or the file pointed to by the `certFile` variable in the old `valicert.ini`)

If present, `default.cert` (or the file pointed to by `defaultSelfCertFile` variable in the old `valicert.ini` file)

If present, `cacrl.cert` (or the file pointed to by the `selfCertFile` variable in the old `valicert.ini`)

`cacrl.req`

Make the following changes in the new `valicert.ini` file:

Set `pkcs11DeviceEnable=1`.

Set `useSoftwareSigning=2`.

Set `pkcs11VendorID` to `1` for Chrysalis or 2 for nCipher.

Set `pkcs11SlotId` to the value of `Chrysalis_SLOT_ID` in the old `valicert.ini` file.

Set `ocspResponsePrivKeyID` to the value of `Chrysalis_RSA_PRIVATE_KEY` in the old `valicert.ini` file.

Set `ocspResponsePubKeyID` to the value of `Chrysalis_RSA_PUBLIC_KEY` in the old `valicert.ini` file.

Make sure the variables in the new `valicert.ini` file point to the files that you copy especially for files that have been renamed.

Step 6 To configure SSL copy the following files from the backed up `entserv` directory to the new `entserv` directory:

`ssl.privkey` (or file pointed to by the `sslPrivateKey` variable in the old `valicert.ini` file).

`sslCert.cert` (or the file pointed by the `sslCertFile` variable in the old `valicert.ini` file).

`ssl.req`

a) For software signing in the `valicert.ini` file, set `sslServerHost` to:

The value of `sslServerHost` in the backed up `valicert.ini`

OR

To a new `host:port`.

b) For SSL hardware signing, copy the following files from the backed up `entserv` directory to the new `entserv` directory:

`sslCert.cert` (or the file pointed by the `sslCertFile` variable in the old `valicert.ini` file).

`ssl.req`

Make the following changes to the `valicert.ini` file:

Set `sslServerHost` to:

The value of `sslServerHost` in the backed up `valicert.ini`.

OR

To a new `host:port`.

Set `sslSigningType = 2`

Set `sslPrivKeyID` to the value of `sslPrivKeyID` in the old `valicert.ini` file.

Set `sslPubKeyID` to the value of `sslPrivKeyID` - 1 in the old `valicert.ini` file.

Step 7 The instructions for upgrading your extensions depends on the extensions you have installed. Install and configure any custom extensions the same way that you initially did (see “Loading the Extension” on page 96).

a) To configure the LDAP extension, follow the instructions below:

Make following changes to the `valicert.ini` file:

For the variable `Enterprise VAExtensions` add the value `./ldapcrl.so`. (If you have no other extensions installed this will be the only value.

Copy the entire `[LdapDirectory]` section from the backed up `valicert.ini` file.

Make following changes to `vcconfig.ini`:

Under the `[DEFAULT]` section, increase the `NO_OF_EXTENSIONS` value by 1.

Copy the corresponding section `[EXTENSION_n]` from the old `vcconfig.ini` file.

Step 8 Copy all the subdirectories under the old `entserv\crls` to the new `entserv\crls` directory.

Step 9 To password protect the new Enterprise VA Administration Server, follow the instructions in “Password Protecting the Enterprise VA Administration Server” on page 38.

Step 10 Restart the Enterprise VA and the Enterprise VA Administration Server.

Step 11 Go to configuration mode and make sure all the trusted CAs certificates are present in the store.

Step 12 Make any desired configuration changes, (see Chapter 4, "Working at the Configuration Mode Menu")

Upgrading from Certificate VA 3.x on UNIX

The following instructions are for using your existing Certificate VA configurations with Enterprise VA 3.2. All of the Enterprise VA settings are configured through the Administration web pages.

To upgrade to ValiCert Enterprise VA on UNIX

Step 1 If necessary, stop the Certificate VA and the Certificate VA Administration Server.

Step 2 Backup the `entserv` directory.

You will use the files in this directory in your Enterprise VA 3.2 installation.

NOTE: After copying any files from the backed up directories make sure to change the user and group to `nobody`. All the files in `entserv` directory are owned by `nobody:nobody`.

In Enterprise VA 3.2, all subdirectories are created under the directory named `va` as opposed to `enterpriseva` in Certificate VA 3.x.

Step 3 Uninstall Certificate VA 3.x and clean the directory.

Remove the Certificate VA Administration Server and the Certificate VA server.

Step 4 Install Enterprise VA 3.2.

Refer to the “Installing Enterprise VA on UNIX” on page 30 for detailed information about installing the Enterprise VA.

Step 5 Copy the following files from the backed up `entserv` directory to the new `entserv` directory:

`ca.cert` (or the file pointed to by the `certFile` variable in the old `valicert.ini`)

If present, `default.cert` (or the file pointed to by `defaultSelfCertFile` variable in the old `valicert.ini`)

If present, `cacrl.cert` (or the file pointed to by the `selfCertFile` variable in the old `valicert.ini`)

`cacrl.privkey` (or the file pointed to by the `privKeyFile` variable in the old `valicert.ini`) `cacrl.req`

NOTE: Some file names specified in the two `valicert.ini` files differ. Make appropriate changes in the new `valicert.ini` file so that the variable values are consistent with the files specified in the old file.

In addition some of the file names are configurable and may be different from the ones shown in this example.

Step 6 To configure SSL copy the following files from the backed up `entserv` directory to the new `entserv` directory:

`ssl.privkey` (or file pointed to by the `sslPrivateKey` variable in the old `valicert.ini` file).

`sslCert.cert` (or the file pointed by the `sslCertFile` variable in the old `valicert.ini` file).

`ssl.req`

Set `sslServerHost` to:

The value of `sslServerHost` in the backed up `valicert.ini`

OR

To a new `host:port`.

Step 7 Copy all the subdirectories under the old `entserv\crls` to the new `entserv\crls`.

Step 8 If you want to password protect the new Enterprise VA Administration Server, follow the instructions in “Password Protecting the Enterprise VA Administration Server” on page 38.

Step 9 Get a new license. To run the Enterprise VA you must have a valid license file. Your Certificate VA license file will not allow you to start the Enterprise VA server. Start the Enterprise VA Administration server.

Step 10 Open your browser and follow the setup instructions for installing a license (see “Getting a Product Key” on page 45).

Step 11 Go to configuration mode and make sure all the trusted CAs certificates are present in the store.

Step 12 Make any desired configuration changes, (see Chapter 4, "Working at the Configuration Mode Menu")

Step 13 Restart the Enterprise VA from the Administration Server On/Off page.

Upgrading from Certificate VA 3.x on NT

To upgrade from Certificate VA, run the installer. The installer detects the Certificate VA and copies the existing configurations to the Enterprise VA. Additional configuration is required, (see Chapter 3, "Setting Up Enterprise VA").

To run the Enterprise VA you must have a valid license file. You must get a new license since your Certificate VA license file will not allow you to start the Enterprise VA server.

Step 1 Install Enterprise VA.

NOTE: If you are prompted to reboot your system at the end of the upgrade, you must do this for the new installation to work. If you are running Enterprise VA as a service you will get an error message on reboot as the service will not run until you get a new license.

Step 2 Open your browser and start the administration server, (see “Accessing the Administration Server” on page 43).

Step 3 Follow the setup instructions for installing a license.

Step 4 Go to configuration mode and make sure all the trusted CAs certificates are present in the store.

Step 5 Make any desired configuration changes, (see Chapter 4, "Working at the Configuration Mode Menu")

Step 6 Restart the Enterprise VA from the Administration Start/Stop Server page.

Installing Enterprise VA on Windows NT

You can install the Enterprise VA on a machine running the Windows NT Server or Windows NT Workstation operating system. Be sure that the machine you plan to install the Enterprise VA software on meets all the system requirements and prerequisites listed in “Before you Begin” on page 7.

NOTE: Before you install the ValiCert Enterprise VA software, be sure to close Microsoft Outlook.

To install the ValiCert Enterprise VA on Windows NT

Step 1 Insert the CD containing the ValiCert Enterprise VA into your CD-ROM drive.

Step 2 Double click on the self-extracting file EVA32Setup.

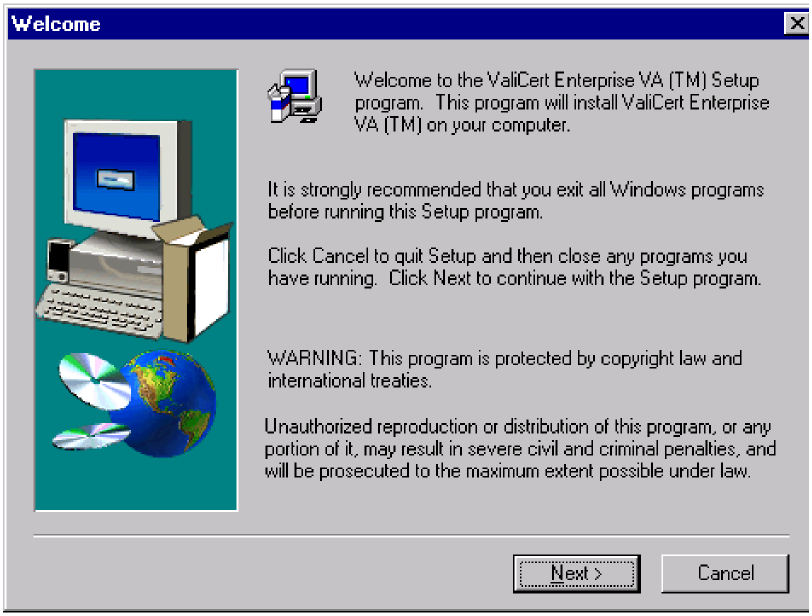
Step 3 The Installation Folder dialog box displays.

Select a folder to extract the installation files into. If the folder does not exist you are prompted to create it.

Step 4 Click **Finish**.

Step 5 The installation files are unpacked and the Setup.exe program launches.

The Install Shield application starts and the Welcome dialog box displays:



Welcome to the ValiCert Enterprise VA (TM) Setup program. This program will install ValiCert Enterprise VA (TM) on your computer.

It is strongly recommended that you exit all Windows programs before running this Setup program.

Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Follow the on-screen instructions as you proceed through the installation.

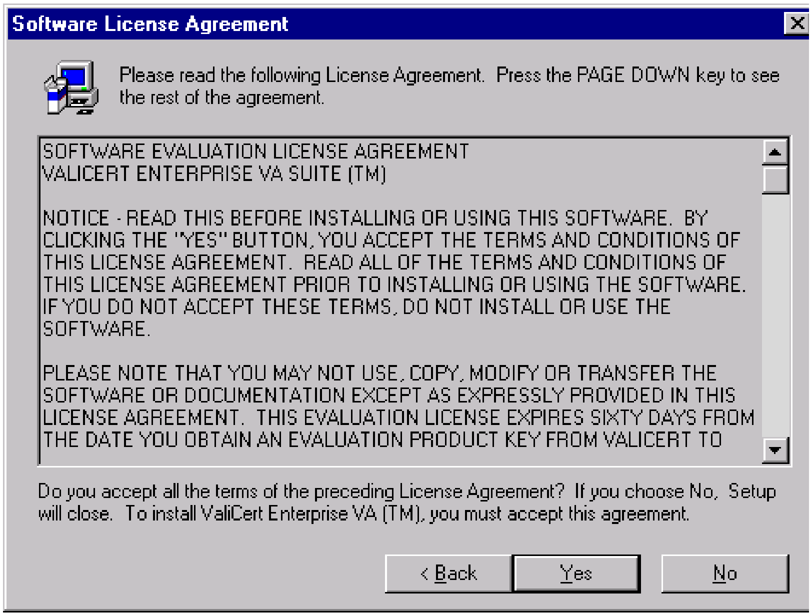
The **Next** button allows you to move forward to the next installation window.

The **Back** button allows you to return to the previous installation window

The **Cancel** button closes the installation program without installing any component of the Enterprise VA. To install Enterprise VA, rerun the installation program.

Step 6 Click **Next.**

The ValiCert Software License Agreement dialog box displays:



Software License Agreement

Please read the following License Agreement. Press the PAGE DOWN key to see the rest of the agreement.

SOFTWARE EVALUATION LICENSE AGREEMENT
VALICERT ENTERPRISE VA SUITE (TM)

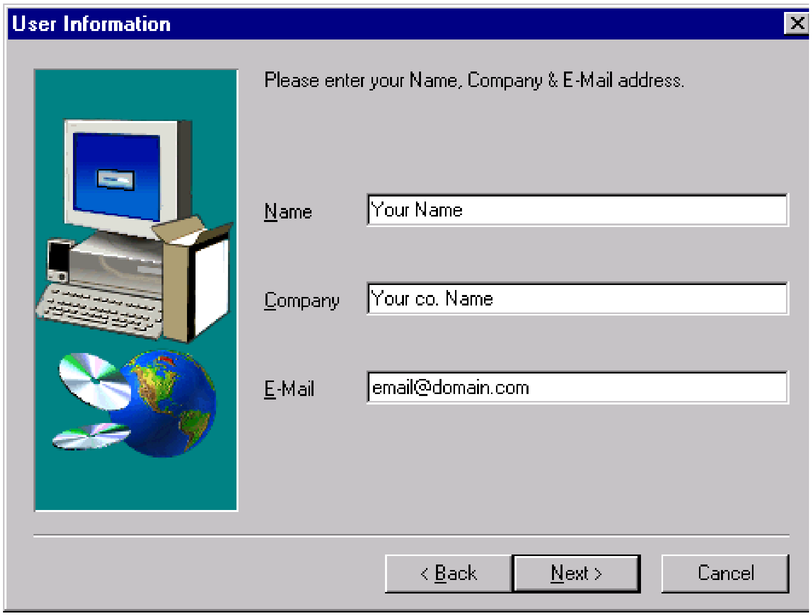
NOTICE - READ THIS BEFORE INSTALLING OR USING THIS SOFTWARE. BY CLICKING THE "YES" BUTTON, YOU ACCEPT THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. READ ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT PRIOR TO INSTALLING OR USING THE SOFTWARE. IF YOU DO NOT ACCEPT THESE TERMS, DO NOT INSTALL OR USE THE SOFTWARE.

PLEASE NOTE THAT YOU MAY NOT USE, COPY, MODIFY OR TRANSFER THE SOFTWARE OR DOCUMENTATION EXCEPT AS EXPRESSLY PROVIDED IN THIS LICENSE AGREEMENT. THIS EVALUATION LICENSE EXPIRES SIXTY DAYS FROM THE DATE YOU OBTAIN AN EVALUATION PRODUCT KEY FROM VALICERT TO

Do you accept all the terms of the preceding License Agreement? If you choose No, Setup will close. To install ValiCert Enterprise VA (TM), you must accept this agreement.

Step 7 Click **Yes** to accept the license agreement.

The User Information dialog box displays:



Name: Your Name

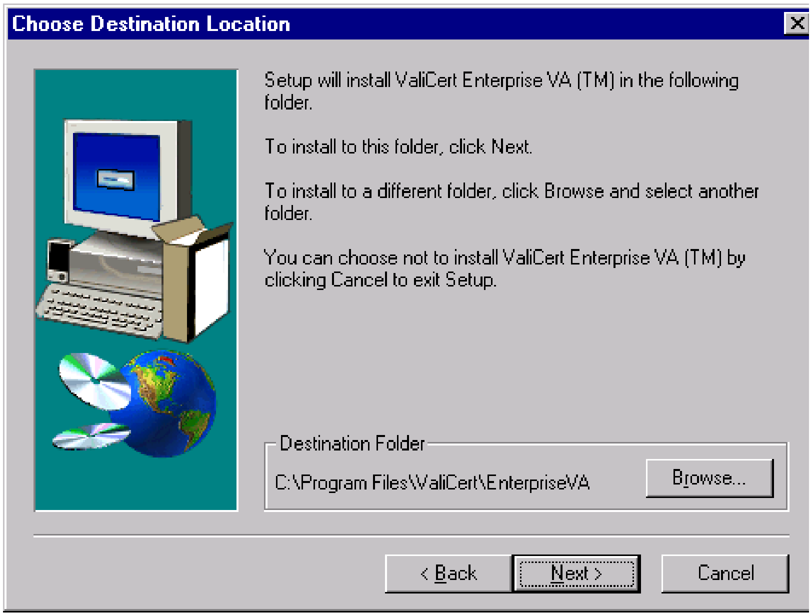
Company: Your co. Name

E-Mail: email@domain.com

Step 8 Type your **Name**, **Company** and **Email ID** (email address) in the text fields provided.

Step 9 Click **Next.**

The Choose Destination Location dialog box displays:



Choose Destination Location

Setup will install ValiCert Enterprise VA (TM) in the following folder.

To install to this folder, click Next.

To install to a different folder, click Browse and select another folder.

You can choose not to install ValiCert Enterprise VA (TM) by clicking Cancel to exit Setup.

Destination Folder

C:\Program Files\ValiCert\EnterpriseVA

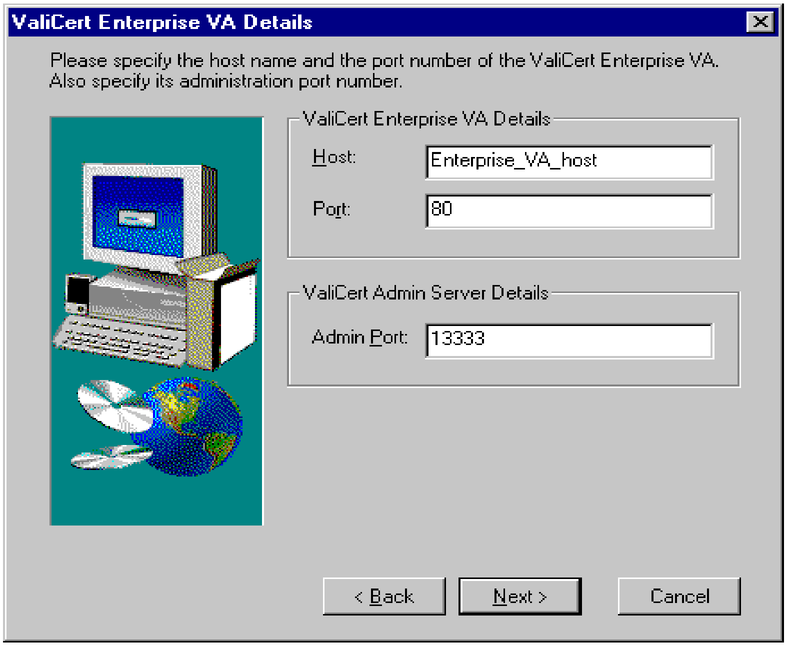
Step 10 Use the default path where the Enterprise VA will be installed.

OR

Use the **Browse** button, if necessary, to navigate to a different folder.

Step 11 Click **Next**.

The ValiCert Enterprise VA Details dialog box displays:



ValiCert Enterprise VA Details

Please specify the host name and the port number of the ValiCert Enterprise VA. Also specify its administration port number.

ValiCert Enterprise VA Details

Host: Enterprise_VA_host

Port: 80

ValiCert Admin Server Details

Admin Port: 13333

Step 12 Enter the host name and port number of the ValiCert Enterprise VA host and the port number of the ValiCert Administration Server.

The ValiCert Enterprise VA host is the machine on which the Enterprise VA will do its work such as process validation requests, receive CRLs, and so forth. Define the following for the ValiCert Enterprise VA host:

Host—The host name identifies the machine. The default host name is the name of the machine on which you are installing the ValiCert Enterprise VA.

Port—The port number identifies the port at which the Enterprise VA host listens and through which information will be transferred to and from the Enterprise VA host. The default port number is 80.

The ValiCert Administration Server is the administration component of the Enterprise VA. You setup and configure the Enterprise VA through this server, which is installed during this installation process. You access the administration server through a browser.

Define the following for the ValiCert Administration Server:

Admin Port—The port number at which the ValiCert Administration Server listens for http requests from the browser. If you use a port other than the default (13333), make a note of the port number for future reference.

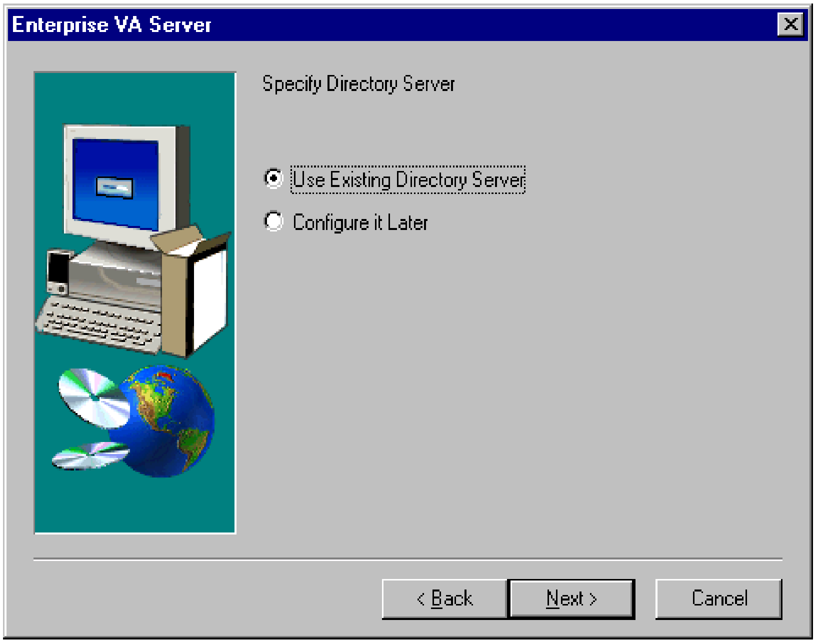
NOTE: If you want to use https requests to communicate configuration decisions to the Administration Server, you must configure this port number manually at the Browser. For more information, see “Using SSL” on page 44.

Step 13 Click **Next**.

The Start Copying Files dialog box displays. Make sure all the information is correct.

Step 14 Click **Next**.

The Enterprise VA Server dialog box displays:



Enterprise VA Server

Specify Directory Server

● Use Existing Directory Server

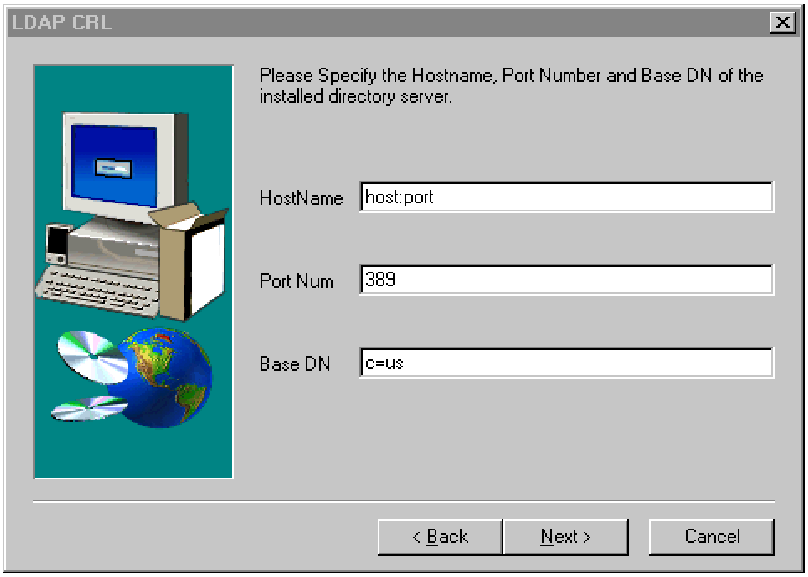
○ Configure it Later

Step 15 Select the Directory Server option that meets your needs.

If you select the **Configure it Later** option:

a) Proceed to step 16.

If you select the **Use Existing Directory Server** option, the LDAP CRL dialog box displays:



LDAP CRL

Please Specify the Hostname, Port Number and Base DN of the installed directory server.

HostName: host:port

Port Num: 389

Base DN: c=us

a) Enter a host name, port number, and base DN for the LDAP Directory Server you want to use.

HostName—specifies the host and port number of the Enterprise VA host. This should match the information you provided in the ValiCert Enterprise VA Details dialog box.

Port Num—specifies the port number at which the LDAP server will be listening for LDAP requests from the LDAP extension. The default port is 389.

Base DN—specifies the root distinguished name in the LDAP directory that you want to store CRLs or CRLDPs. The recommended values are c=us or a null string (“ “).

b) Proceed to step 16.

Step 16 Click **Next**.

Files are copied from the CD to the specified destination location.

The Setup Complete dialog box displays.

To read the latest ValiCert Enterprise VA information now, select **Yes, I want to view the Readme File**.

To start the Enterprise VA Administration Server now, select **Yes, I want to launch Admin Console**.

Step 17 Click **Finish**.

After the installation is complete, your selections at the Setup Complete dialog box determine whether the Readme file opens and whether your default browser opens displaying the administrative page of the ValiCert Enterprise VA that you installed.

The setup program adds **ValiCert Enterprise VA** to your **Start** menu. You can access the ValiCert Enterprise VA Readme file, administration page, and configuration setup page from the Start menu.

You are now ready to use the administrative interface to configure and manage the Enterprise VA.

Proceed to Chapter 3, "Setting Up Enterprise VA"

Installing Enterprise VA on UNIX

Install the Enterprise VA on a UNIX machine running Solaris 2.6 or 2.7.

NOTE: To use the Netscape browser after installing the Enterprise VA, change the browser’s default font to Helvetica. Otherwise, unexpected results in your browser displays may occur.

To install the ValiCert Enterprise VA on UNIX

Step 1 Log in as root on the machine where you want to install the Enterprise VA.

Step 2 Insert the CD containing the Enterprise VA into your CD-ROM drive.

Step 3 Open a shell window and enter the following at the command line prompt to uncompress the packages:

```
tar xvf EVA32setup.tar
```

Step 4 Type the following at the command line prompt to display the packages:

```
/usr/bin/pkgadd -d installers
```

The **pkgadd** menu displays:

```
The following packages are available:
 1  VCadmin     ValiCert Enterprise VA Administration Server
                (sparc) 3.2
 2  VCeva       ValiCert Enterprise VA
                (sparc) 3.2
 3  VCpub       ValiCert VA Publisher
                (sparc) 3.2
 4  VCval       ValiCert Netscape Web Server Validator
                (sparc) 3.2
Select package(s) you wish to process (or ‘all’ to process
all packages). (default: all [?,??,q]:
```

To cancel the installation at any time, type **q** and press [Enter] at the command prompt.

NOTE: You must always install the ValiCert Enterprise VA Administration Server package first, followed by the ValiCert Enterprise VA package. The sequence in which you install the remaining packages is not critical.

Step 5 Type **1** and press [Enter] to install <VCadmin>, the Enterprise VA Administration Server package.

The following displays:

```
Where do you want to install the Enterprise VA admin server
(Path will be created if it does not exist)?
Default: /usr/local/valicert [?,q]
```

Step 6 Type the <VAInstallDir> location and press [Enter] or press [Enter] to accept the default.

If you specify a <VAInstallDir> location, use the full path of the location where you want the ValiCert Administration Server installed. The default <VAInstallDir> location is `/usr/local/valicert`.

When it is successfully installed the following message displays:

```
Installation of <VCadmin> was successful.
The following packages are available:
 1  VCadmin    ValiCert Enterprise VA Administration Server
               (sparc) 3.2
 2  VCeva      ValiCert Enterprise VA
               (sparc) 3.2
 3  VCpub      ValiCert VA Publisher
               (sparc) 3.2
 4  VCval      ValiCert Netscape Web Server Validator
               (sparc) 3.2
Select package(s) you wish to process (or 'all' to process
all packages). (default: all [?,??,q]:
```

Step 7 Type **2** and press [Return] to install <VCeva>, the Enterprise VA package.

The ValiCert license agreement displays along with the following prompt:

```
Do you agree to the terms of this license agreement Yes or
No [y,n,?,q]
```

Step 8 Type **y** and press [Return].

The following displays:

```
Enter the port number for the Enterprise VA Admin Server.
Default: 13333 [1-33333,?,q]
```

NOTE: If you have already installed this version of the Enterprise VA, the following message displays:

```
This appears to be an attempt to install the same
architecture and version of a package which is
already installed. This installation will attempt
to overwrite this package.
```

Step 9 Press [Enter] to accept the default Admin Server port or type a port number and press [Enter].

This port number identifies the port at which the ValiCert Administration Server listens and through which your configuration decisions will be sent to and received from the browser in http requests.

The ValiCert Administration Server is the administration component of the Enterprise VA. This server, which is installed during this installation process, handles all the configuration decisions that you will make at the various dialog boxes for the ValiCert Enterprise VA. If you choose to use a port other than the default, make a note of the port number for future reference.

NOTE: If you want to use https requests to communicate configuration decisions to the Administration Server, you must configure this port number manually at the Browser. For more information, see "Using SSL" on page 44.

The following displays:

```
Enter the port number for the EVA. Default: 80 [1-65535,?,q]
```

Step 10 Press [Enter] to accept the default Enterprise VA port or type in a port number and press [Enter].

This port number identifies the port at which the Enterprise VA Host listens and through which information will be transferred to and from the Enterprise VA Host.The ValiCert Enterprise VA Host is the machine on which the Enterprise VA will do its work such as process validation requests, receive CRLs, and so forth. The default port number is 80.

NOTE: The ValiCert Enterprise VA host port information corresponds to the port portion of the serverHost parameter of the [ves] section of the `valicert.ini` file.

The following displays:

```
Enter the e-mail address of the server administrator. [?,q]
```

Step 11 Enter an e-mail address and press [Enter].

The Enterprise VA Admin Server uses this e-mail address to send informational messages to the server administrator during configuration and administration performed at the Enterprise VA dialog boxes.

The following displays:

```
Enter the server’s host name (either a registered DNS name
or an IP address): [?,q]
```

Step 12 Enter a host name and press [Enter].

The host name identifies the machine on which you have installed the Enterprise VA.

The following displays:

```
Enter the user name to run the Admin Server as:
```

Step 13 Enter **nobody** and press [Enter].

The following displays:

```
##Executing checkinstall script
Prerequisite VCadmin package installed
Using </usr/local/valicert> as the package base directory
##Processing package information.
##Processing system information.
  6 package pathnames are already properly installed
##Verifying package dependencies.
##Verifying disk space requirements.
##Checking for conflicts with packages already installed.
##Checking for setuid/setguid programs.

This package contains scripts which will be executed with
super-user permission during the process of installing this
package.

Do you want to continue with the installation of <VCeva>
[y,n,?]
```

Step 14 Enter **y** and press [Enter] to continue to install the <VCeva> package.

The package installs.

When it is successfully installed the following message displays:

```
Installation of <VCadmin> was successful.
The following packages are available:
 1  VCadmin    ValiCert Enterprise VA Administration Server
               (sparc) 3.2
 2  VCeva      ValiCert Enterprise VA
               (sparc) 3.2
 3  VCpub      ValiCert VA Publisher
               (sparc) 3.2
 4  VCval      ValiCert Netscape Web Server Validator
               (sparc) 3.2
Select package(s) you wish to process (or ‘all’ to process
all packages). (default: all [?,??,q]:
```

The pkgadd script installs the EVA Administration Server in a directory called va within the default installation directory or the one you specified.

Step 15 Enterprise VA is now installed. Type **q** and press [Enter].

The installation script is stopped and you are returned to the command prompt.

NOTE: If you want to install other packages continue to select the appropriate number and press [Enter]. Follow the on-screen instructions. Refer to the appropriate manual for detailed instructions on how to install these other packages.

You are now ready to password protect the Enterprise VA Administration Server.

Proceed to “Password Protecting the Enterprise VA Administration Server” on page 38.

Starting the Administration Server on UNIX

After you install the VCadmin and VCeva packages, you can start the Enterprise VA Administration Server so that you can configure the Enterprise VA. The Enterprise VA Administration Server can be accessed through a browser after you start the server.

To start the Enterprise VA Administration Server on UNIX

Step 1 Type the following command to change to the correct directory

```
cd <VAInstallDir>/va/apache/bin/
```

Step 2 Type the following command to start the Enterprise VA Administration Server:

```
./apachectl start
```

NOTE: The `<VAInstallDir>` parameter is the full path you specified in step 6 or the default location `/usr/local/valicert`.

Step 3 Type the following command to check if the process is running:

```
ps -ef | grep apache
```

You will see one or more lines similar to the following:

```
nobody 9022 9020 0 14:18:30 0:00
../../apache/bin/httpd
```

You are now ready to configure the Enterprise VA using the Enterprise VA Administration Server user interface.
The administrative interface is Web-based, and is accessed through the URL `http://<host>:<port>`, where `host` and `port` are the ValiCert Enterprise VA host name and port number you provided during installation.

Removing a ValiCert Package from UNIX

You can remove any of the ValiCert packages from your UNIX machine

To remove a package

Step 1 Enter the following at the command prompt and press [Return]:

```
pkgrm <packagename>
```

The <packagename> parameter can be any of the following:

VCadmin

VCeva

VCpub

VCval

Text similar to the following displays, depending on the package you want to remove:

```
The following package is currently installed:
VCeva ValiCert Enterprise VA
 (sparc) 3.2

Do you want to remove this package?
```

Step 2 Enter **y** and press [Return] to remove the package.

When the removal is complete the following message displays:

```
Removal of <packagename> was successful.
```

Password Protecting the Enterprise VA Administration Server

The Enterprise VA Administration Server can be run and managed locally or remotely. This means that any machine that accesses the server machine can run the Administration Server. To ensure that only authorized users access the Enterprise VA Administration Server, password protect it.

To password protect your Enterprise VA Administration Server

Step 1 Create an Authorized User file using the `htpasswd` utility.

On UNIX, the `htpasswd` utility is in the `../apache/bin` directory. Type the following:

```
../bin/htpasswd -c <filename> <username>
```

On Windows NT, the `htpasswd` utility is in the `<installation directory>\EnterpriseVA\Apache` directory. Type the following:

```
httpasswd.exe
```

NOTE: You can only create one user at a time. This means that if you want to have more than one authorized user, you need to repeat this command for each user you want to add to the Authorized User file.

Step 2 Enter the password for the user you are creating and confirm it.

Step 3 Create a Group file using a text editor (like `vi`).

The Group file must contain at least one group and one user. The group file must contain entries in the following format:

```
<groupname>:<username>
```

Step 4 Edit the `httpd.conf` file to include the following lines in the `<Directory>` section for the document's folder such as `<Directory/usr/local/valicert/va/apache/htdocs>:`

```
AuthType Basic
AuthName <name>
AuthUserFile <filename>
AuthGroupFile <filename>
require group <groupname>


</Directory>
```

The parameters in the file are as follows:

AuthType Basic—specifies that Basic password protection is to be employed.

AuthName <name> —specifies the label you want the password dialog box to display when a user tries to access the Administration Server. It can be any number of characters, however, if you want to include spaces, be sure to use quotation marks.

AuthUserFile—specifies the full path name of the AuthFile you created in step 1 using the `httpasswd` utility.

AuthGroupFile—specifies the full path name of the group file you created in step 3 using an editor such as `vi`.

require group—specifies the group to which a user must belong in order to access the Administration Server.

The following is an example of the entries that need to be made in the `httpd.conf` file.

```
AuthType Basic
AuthName “EVA 3.2 Administration”
AuthUserFile va/apache/conf/authfile
AuthGroupFile va/apache/conf/groupfile
require group admin
```

You are now ready to start the Enterprise VA Administration server.

Uninstalling Enterprise VA for NT

To remove Enterprise VA for NT

In the Start Menu

Select Start > Programs > ValiCert Enterprise VA > Uninstall ValiCert Enterprise VA

OR

Run the `VesUninst.exe` program in the installation directory.

If the program does not exist, delete the entire installation directory.

CHAPTER 3

Setting Up Enterprise VA

This section explains how to set up and configure the Enterprise VA. Enterprise VA is configured through the graphical user interface (GUI) of the ValiCert Administration Server. The GUI provides a Setup menu which guides you through the tasks necessary to set up the Enterprise VA after you install it.

For information about the options available after starting the Enterprise VA, see Chapter 4, "Working at the Configuration Mode Menu."

NOTE: The GUI for Windows NT and UNIX are identical except that from the Windows NT version you are able to start and stop the server. You are not able to do this from the UNIX version. Because the interfaces are otherwise identical, screen shots from the Windows NT version are provided to guide you through the configuration process.

Although the Administration Server interface steps you through a series of configuration tasks, you are not required to configure the Enterprise VA in this sequence.

Setting Up the ValiCert Enterprise VA

This section provides an overview of the tasks you can perform at the Setup menu. After you complete each task, the **Next Step** link is displayed. Click this link to follow the recommended path for first time configuration of the Enterprise VA.

To set up the ValiCert Enterprise VA

Step 1 Access the ValiCert Enterprise VA Administration Server interface.

For information about this step, see “Accessing the Administration Server” on page 43.

Step 2 Get a ValiCert Enterprise VA product key.

The ValiCert Enterprise VA requires a product key, which entitles you to a free 60-day evaluation period. If you purchase the product, you will receive a permanent product key from ValiCert. For information about this step, see “Getting a Product Key” on page 45.

Step 3 Add Extensions.

The Enterprise VA allows you to add extensions. For information about the extensions that ValiCert provides, see Built-in Extensions. For information about using the Extension API to create your own extension, see Creating Your Own Extension. For detailed information about this step, see “Adding Extensions” on page 48.

Step 4 Create a public/private key pair for the ValiCert Enterprise VA.

You will use the key pair to obtain a certificate for your server. The certificate is used to establish your server's identity to applications that contact the server. For information about this step, see “Creating Key Pairs” on page 51.

Step 5 Add the CA root certificate.

To validate certificate revocation lists (CRLs) issued from a CA, you must add the CAs root certificate to your ValiCert Enterprise VA's certificate repository. Instructions are provided for both the Netscape CMS, and the Microsoft Certificate Server. You can add several certificates, if necessary. For information about this step, see “Adding the CA Root Certificate” on page 58.

Step 6 Modify the ValiCert Enterprise VA configuration.

You can specify values for various parameters for the server. However, the default parameters should be sufficient for most users. For information about this step, see “Modifying the Enterprise VA Configuration” on page 67.

Step 7 Configure extensions.

You can configure the extensions that you added earlier in Step 3. For information about this step, see “Configuring and Deleting Extensions” on page 71.

Step 8 Start or stop the Enterprise VA.

For information about this step, see “Starting and Stopping the Enterprise VA Server on Windows NT” on page 72.

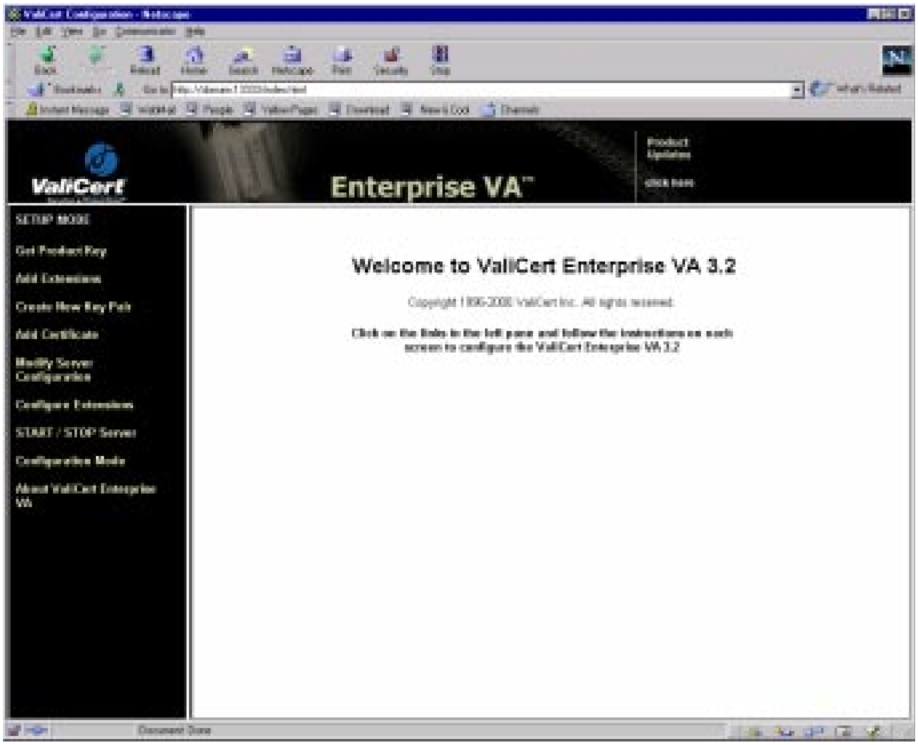
Accessing the Administration Server

The Administration Server interface requires the installation of an HTTP server, which is automatically installed and configured during the ValiCert Enterprise VA installation. You can launch the Administration Server interface automatically during installation or you can access it through the following URL:

```
http://<host>:<port>
```

where `<host>` and `<port>` are the ValiCert Enterprise VA administration host name and port number you provided during installation.

When you access the Administration Server through the Administration Server interface, the following screen displays.



Welcome to ValiCert Enterprise VA 3.2

Copyright 1996-2000 ValiCert Inc. All rights reserved.

Click on the links in the left pane and follow the instructions on each screen to configure the ValiCert Enterprise VA 3.2

To use SSL, see "Using SSL" below.

Using SSL

You can send your Enterprise VA configuration requests between the browser and the Administration server over a secure connection using Netscape's Secure Socket Layer (SSL). SSL encrypts and decrypts all configuration requests that you make through the web-based Enterprise VA user interface and all the responses you receive from the Administration Server. SSL, by default, uses port 443.

To use SSL, specify a URL and port preceded by `https` similar to the following at your browser:

```
https://www.domain.com:443
```

For information about setting up a secure session, see Appendix C, "Security for VA Administration."

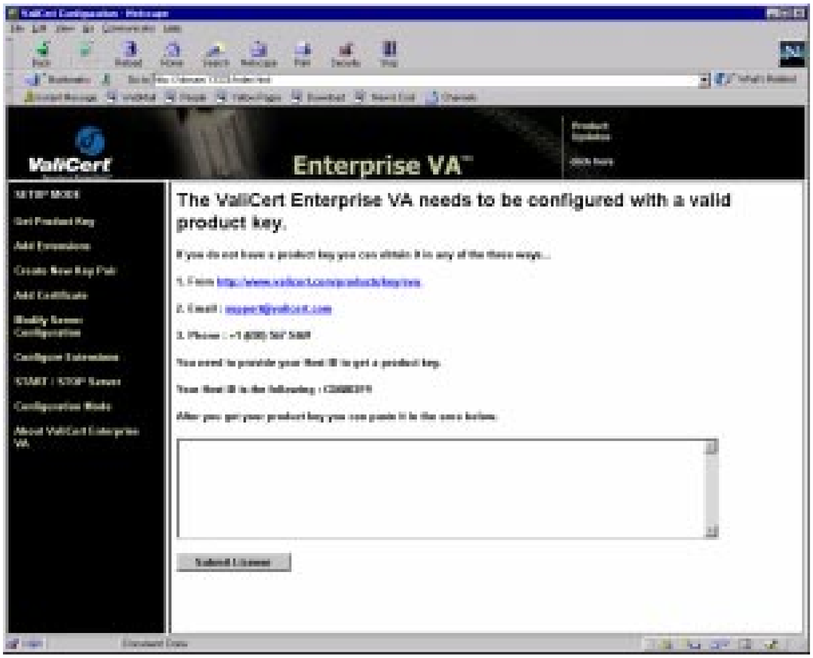
Getting a Product Key

To use the ValiCert Enterprise VA, you need a product key.

To get a product key

Step 1 Click **Get Product Key** in the main Administration Server page.

The product key page displays:



The ValiCert Enterprise VA needs to be configured with a valid product key.

If you do not have a product key you can obtain it in any of the three ways...

1. From http://www.valicert.com/[illegible]

2. Email : support@valicert.com

3. Phone : +1 [illegible]

You need to provide your Host ID to get a product key.

Your Host ID is the following : [illegible]

After you get your product key you can paste it in the area below.

Step 2 To get the product key either connect to the ValiCert web site for a trial license or contact ValiCert by phone or email for a permanent license.

Use one of the following methods:

a) To get a 60-day trial license, note your `hostid`.

Click `http://www.valicert.com/products/key/eva`. The ValiCert Product Evaluation Key Center page displays.

On this page, enter the requested information, including your `hostid` (from the previous page).

Select whether you want to be on the ValiCert mailing list.

Click **Submit Request**.

A page displaying your product key opens. Copy the license information to the Clipboard.

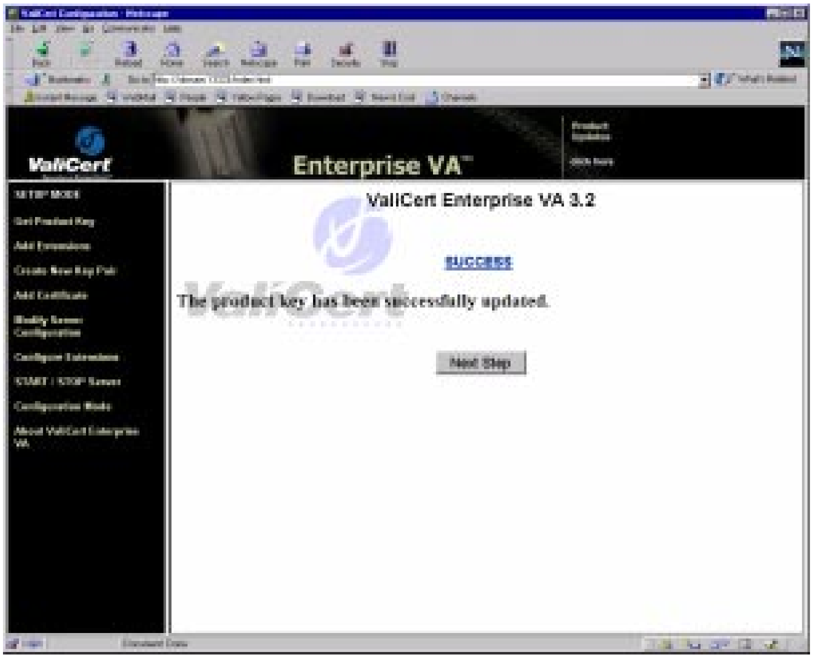
b) Send e-mail to `support@valicert.com`. Be sure to include your `hostid` in the body of the message.

c) Call ValiCert at the number listed on the page. Be sure you have your `hostid` available when you call.

Step 3 Paste the license text into the product key area of the Get Product Key page.

Step 4 Click **Submit License**.

The following page displays.



ValiCert Enterprise VA 3.2

SUCCESS

The product key has been successfully updated.

Step 5 If you are only installing a new product key and you have already configured the VA, restart the server to use the Enterprise VA with the settings you specified previously. (See “Starting and Stopping the Enterprise VA Server on Windows NT” on page 72 or “Starting and Stopping the Enterprise VA Server on UNIX” on page 74.)

OR

To proceed with the next step for first time configuration click **Next Step**. The next step is Adding Extensions.

Adding Extensions

The Enterprise VA Administration Server interface by default allows you to add the LDAP and OCSP ValiCert extensions. However, for purposes of demonstrating the process, the LDAP extension will be added.

If you have created you own extension using the Extension API, you can also add your own extensions through this interface.

NOTE: For Windows NT, if you want to add and manage your own extension through the Administration Server, be sure that its `.ecf` file and `.dll` are located in the following directory:

```
<VAInstallDir>/va/entserv
```

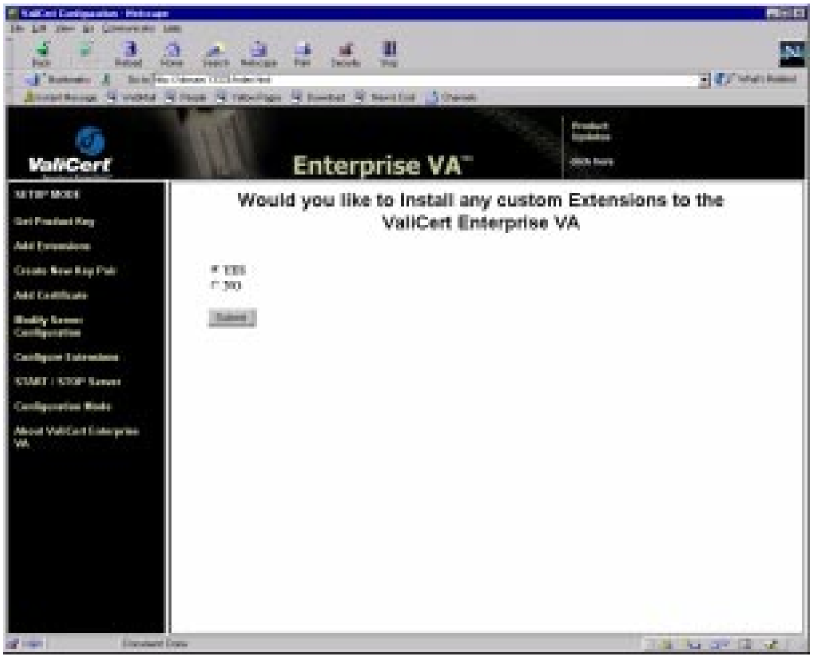
For UNIX, be sure its `.ecf` file and `.so` are located in the following directory:

```
<VAInstallDir>/va/entserv
```

To add an extension

Step 1 Click **Next Step** from the product key page if you are working in sequence, or click **Add Extensions** from the Setup menu.

If you are working in sequence (clicked **Next Step** from the product key successfully added page) the following Extensions web page displays:



Would you like to Install any custom Extensions to the ValiCert Enterprise VA

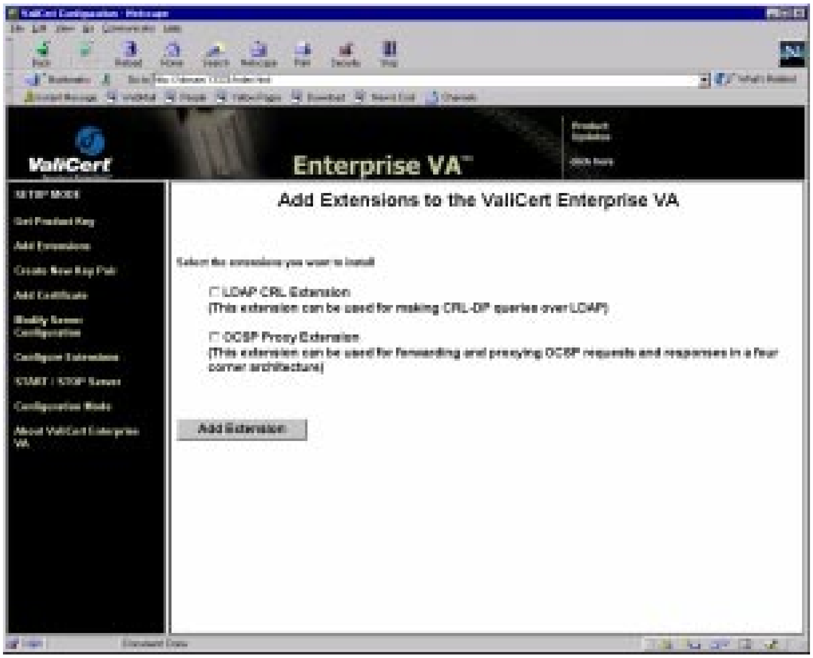
● YES
○ NO

Step 2 Select the **Yes** and click **Submit** to install an extension.

OR

To skip this step and proceed to generating a key pair, select **No** and click the **Submit** button.

The Add Extensions web page displays.



Add Extensions to the ValiCert Enterprise VA

Select the extensions you want to install

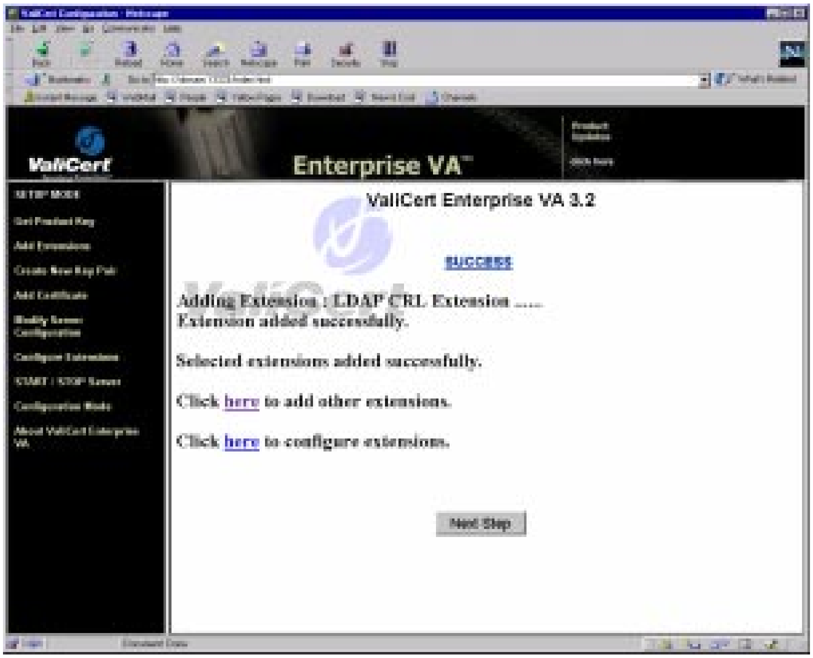
□ LDAP CRL Extension
(This extension can be used for making CRL-DP queries over LDAP)

□ OCSP Proxy Extension
(This extension can be used for forwarding and proxying OCSP requests and responses in a four corner architecture)

By default, the Administration Server interface lists the ValiCert extensions. If you have added your own extension, this page can include your extensions.

Step 3 Select the extension(s) you want to add and click **Add Extension**.

The following extensions page displays:



ValiCert Enterprise VA 3.2

SUCCESS

Adding Extension : LDAP CRL Extension .....
Extension added successfully.

Selected extensions added successfully.

Click here to add other extensions.

Click here to configure extensions.

Step 4 To configure the extension(s) click **Configure**

OR

To continue with the series of steps for first time configuration click **Next Step**. The next step is Creating a New Key Pair.

Creating Key Pairs

Enterprise VA uses keys for signing responses and requests and for SSL communication.

To run the Enterprise VA you must generate a private key for signing OCSP/CRT requests and responses. When you generate a private key an associated public key is also generated. The public key is incorporated into a certificate, either self-signed or delegated (signed by a public CA), which is used for authentication.

The public/private key pair for your server is used to generate a certificate signing request for your ValiCert Enterprise VA. Submit the certificate signing request to a CA to get a delegated certificate.

Generate key pairs with a software-based or hardware-based mechanism through the Enterprise VA's administration system. Software key pairs are generated by the Enterprise VA.

NOTE: The software-based method requires you to use Netscape Communicator 4.7 or later and Microsoft Internet Explorer 5.01 or later.

Hardware key pairs are generated by an external PKCS#11 device. For instructions on creating key pairs with hardware, see “Generating Hardware Keys” on page 150.

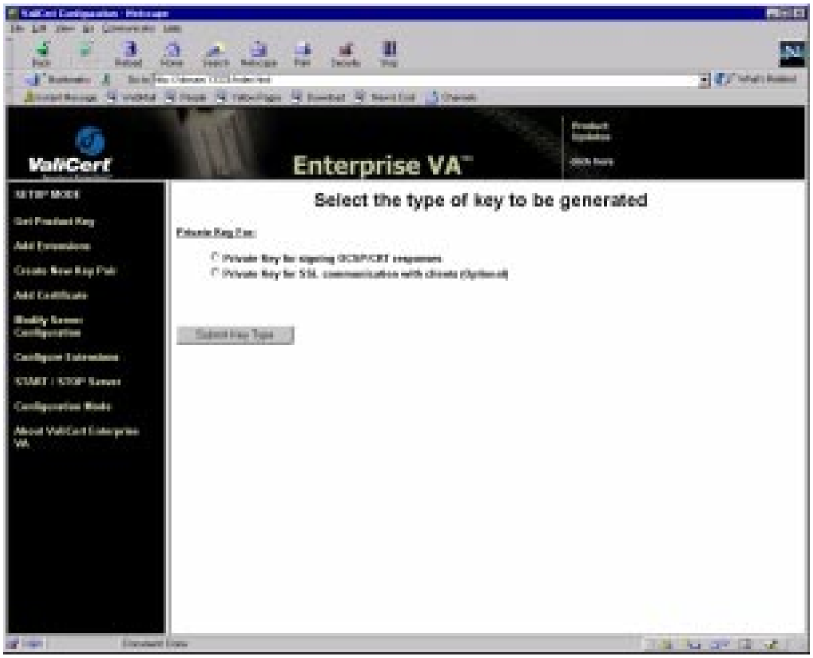
NOTE: Enterprise VA does not support a mixture of hardware and software signing mechanisms.

Creating Software Key Pairs

To create a new software key pair

Step 1 If necessary, click **Create New Key Pair** from the Setup menu to display the key pair page.

The key pair web page displays:



Select the type of key to be generated

Private Key For:

○ Private Key for signing OCSP/CRT responses

○ Private Key for SSL communication with clients (Optional)

NOTE: If you have added extensions, more key types may be available.

Step 2 Select a key type and click **Submit Key Type**.

NOTE: The Private Key for signing OCSP/CRT responses is required by the Enterprise VA.

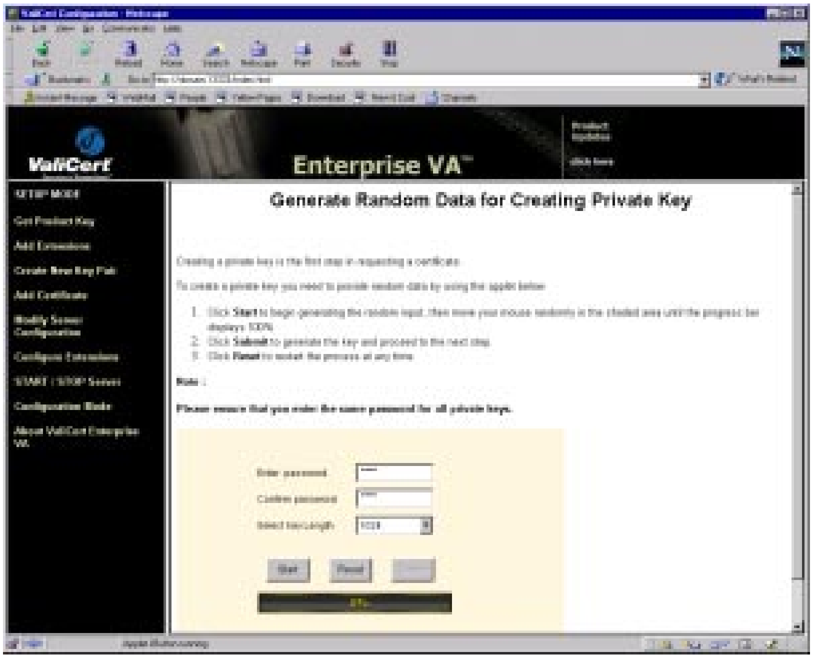
The Private Key for SSL communication with clients is optional but is required for SSL communication.

The page that displays next depends on whether the key exists or not.

If the key you are generating exists, select **Backup** or **Overwrite** and click **Submit Key Generation Technique**.

NOTE: Backup will save the existing key (in the `<VAInstallDir>/entserv/backupkey` directory with a time stamp in the file name.)

The following web page displays:



Generate Random Data for Creating Private Key

Creating a private key is the first step in requesting a certificate.

To create a private key you need to provide random data by using the applet below.

1. Click **Start** to begin generating the random input, then move your mouse randomly in the shaded area until the progress bar displays 100%.
2. Click **Submit** to generate the key and proceed to the next step.
3. Click **Reset** to restart the process at any time.

Note :

Please ensure that you enter the same password for all private keys.

Enter password ****

Confirm password ****

Select key length 1024

Step 3 Enter and confirm the **password** you will use to protect your private key.

NOTE: The password used for all private keys must be the same.

Step 4 Choose a value from the **Select key length** list box.

A key length of 1024 bytes should be sufficient for most applications.

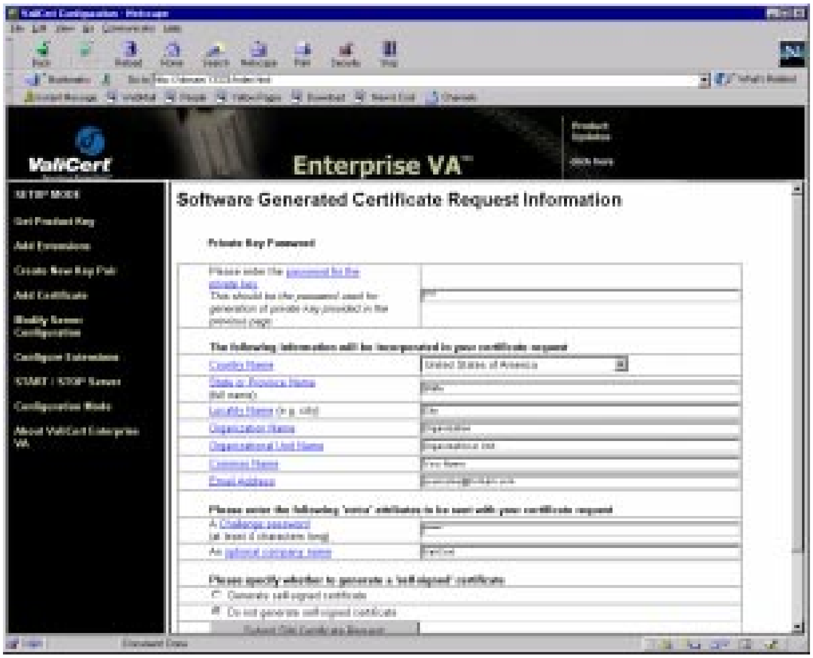
Step 5 Click **Start** and move the cursor randomly in the shaded area until the progress indicator displays 100%.

The cursor movement creates random data that is used to generate the key.

To stop this operation at any time click **Reset**.

Step 6 Click **Submit**.

The Software Generated Certificate Request Information page displays:



Software Generated Certificate Request Information

Private Key Password

Please enter the password for the private key. This should be the password used for generation of private key provided in the previous page.	[illegible]
The following information will be incorporated in your certificate request	
Country Name	United States of America
State or Province Name (full name)	[illegible]
Locality Name (e.g. city)	[illegible]
Organization Name	[illegible]
Organizational Unit Name	[illegible]
Common Name	[illegible]
Email Address	[illegible]
Please enter the following 'extra' attributes to be sent with your certificate request	
A Challenge password (at least 4 characters long)	[illegible]
An optional company name	[illegible]

Please specify whether to generate a 'self-signed' certificate

○ Generate self-signed certificate

● Do not generate self-signed certificate

Step 7 The Enterprise VA generates a certificate request. You can also generate a self-signed certificate.

Enter the certificate request information.

Password: Type the password that you specified earlier to protect the private key. You will need to use this password every time you start the ValiCert Enterprise VA.

Country Name: Select the name of the country in which the server resides.

State or Province Name: Type the full name of the state or province in which the server resides.

Locality Name: Type the full name of the city in which the server resides.

Organization Name: Type the full name of the organization that “owns” the server, for example, Acme Corporation.

Organizational Unit Name: Type the full name of the unit within the organization that “owns” the server, for example, “Electronic Commerce Division.”

Common Name: Type the URL of the server, for example `http://computer.domain.com:1333/`.

E-Mail Address: Type the e-mail address of the server’s administrator.

Challenge Password: Type a password that you will use when retrieving the signed certificate. This password must be at least four characters long.

Optional Company Name: Type the company name, without using any spaces between characters.

Generate self-signed certificate: Select this option to generate a self-signed certificate.

The ValiCert Enterprise VA uses its self-signed certificate to sign validation responses. In this model, the client application needs to have both the CA root certificate and the ValiCert Enterprise VA root certificate in order to read the responses.

Do not generate self-signed certificate: Select this option to only generate a certificate request.

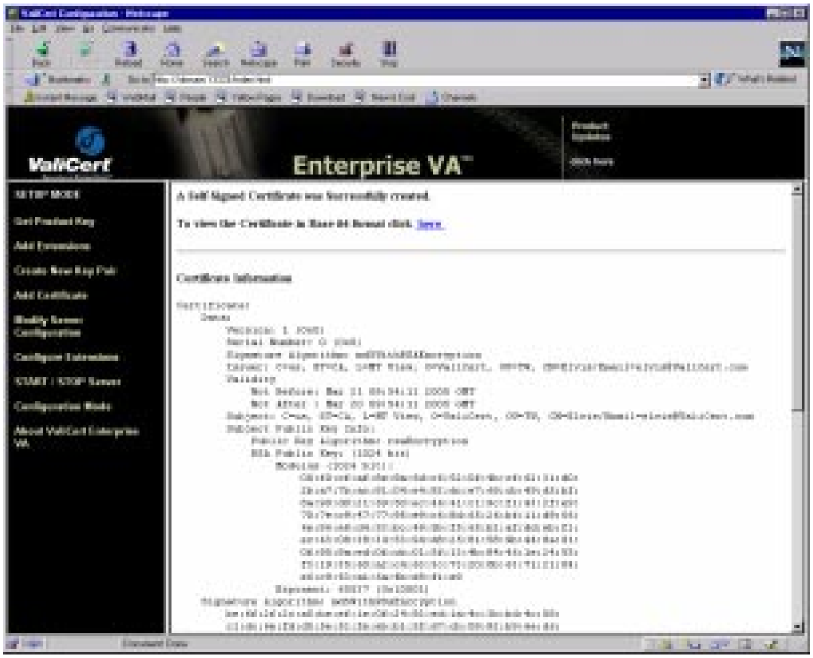
You must install the certificate you get from the CA after you submit the request. In this model, the ValiCert Enterprise VA uses a certificate signed by a CA to sign validation responses. This indicates that the ValiCert Enterprise VA is trusted by the CA to validate certificates. In this case, the client application only needs the CA root certificate in order to trust the responses.

NOTE: To use a certificate signed by a CA, proceed to Appendix A, "Using Delegated Certificates." Do this prior to completing the remaining configuration tasks.

Step 8 Click **Submit SW Certificate Request**.

NOTE: This certificate is stored as `default.cert` in your `entserv` directory.

A web page containing the self-signed certificate information displays:



A Self Signed Certificate was Successfully created.

To view the Certificate in Base 64 format click here.

Certificate Information

```
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number: 0 (0x0)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: [illegible]
        Validity
            Not Before: [illegible]
            Not After : [illegible]
        Subject: [illegible]
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    [illegible]
                Exponent: 65537 (0x10001)
    Signature Algorithm: md5WithRSAEncryption
        [illegible]
```

Step 9 To proceed with the next step for first time configuration click **Next Step**. The next step is Adding the CA Root Certificate.

Adding the CA Root Certificate

Before the ValiCert Enterprise VA can verify CRLs from a CA, you must add the CA’s root certificate to your certificate repository. This section describes how to obtain and add a root certificate from a local CA to the Enterprise VA certificate store. For general instructions on adding certificates see “Adding Certificates to a Store” on page 84.

The method you use to obtain the CA’s root certificate, depends on the certificate server you use. You can use any certificate server.

Examples for using the following certificate servers are provided:

- Netscape Certificate Management System (CMS) 4.1
- Microsoft Certificate Server 1.0

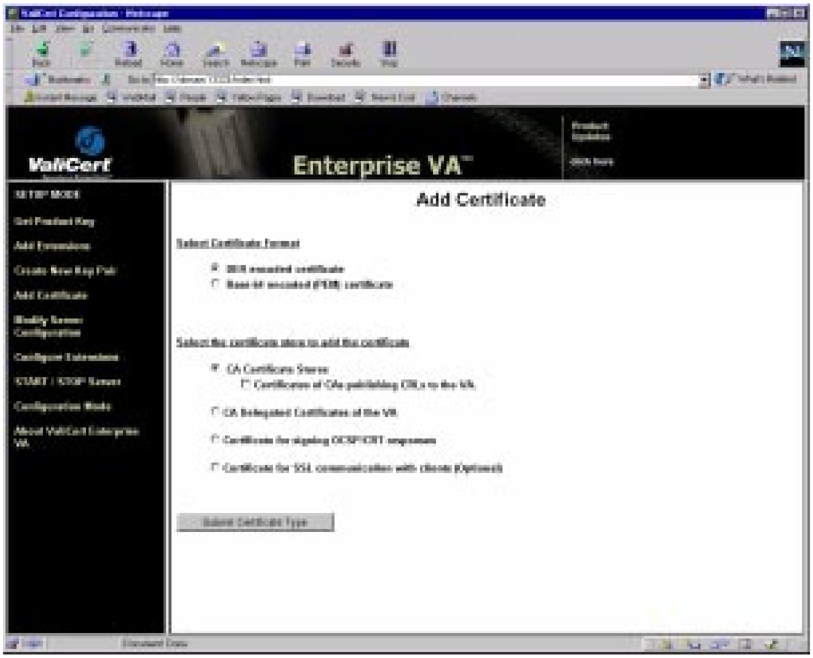
These are provided as examples of how to add a root CA certificate to the Enterprise VA.

Using the Netscape CMS 4.1 to Add Certificates

To add the CA root certificate using Netscape CMS

Step 1 Click **Next Step** from the certificate information page if you are working in sequence, or click **Add Certificate** from the Setup menu.

The Add Certificate web page displays.



Add Certificate

Select Certificate Format

● DER encoded certificate
○ Base 64 encoded (PEM) certificate

Select the certificate store to add the certificate

● CA Certificate Stores
□ Certificates of CAs publishing CRLs to the VA
○ CA Delegated Certificates of the VA
○ Certificate for signing OCSP/CRT responses
○ Certificate for SSL communication with clients (Optional)

Step 2 Select the certificate format you want. For Netscape CMS 4.1, select Base 64 encoded (PEM) certificate (e.g. issued by Netscape Certificate Server).

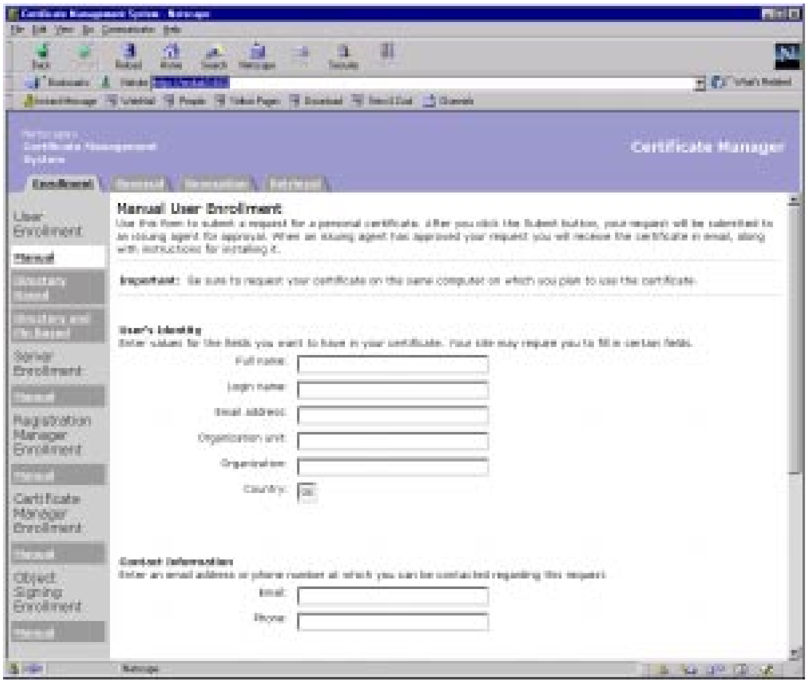
Step 3 Select the certificate store to which you want to add the certificate. (To add a certificate of a CA that publishes CRLs to the VA, select Certificates of CAs publishing CRLs to the VA.)

Step 4 Click **Submit Certificate**.

Step 5 Open another browser window.

Step 6 Enter the URL for the main Netscape CMS 4.1 page, for example `https://NetscapeCMShost:443/`.

The Main page for the Netscape CMS Server 4.1 displays.



Manual User Enrollment

Use this form to submit a request for a personal certificate. After you click the Submit button, your request will be submitted to an issuing agent for approval. When an issuing agent has approved your request you will receive the certificate in email, along with instructions for installing it.

Important: Be sure to request your certificate on the same computer on which you plan to use the certificate.

User's Identity

Enter values for the fields you want to have in your certificate. Your site may require you to fill in certain fields.

Full name:

Login name:

Email address:

Organization unit:

Organization:

Country: US

Contact Information

Enter an email address or phone number at which you can be contacted regarding this request.

Email:

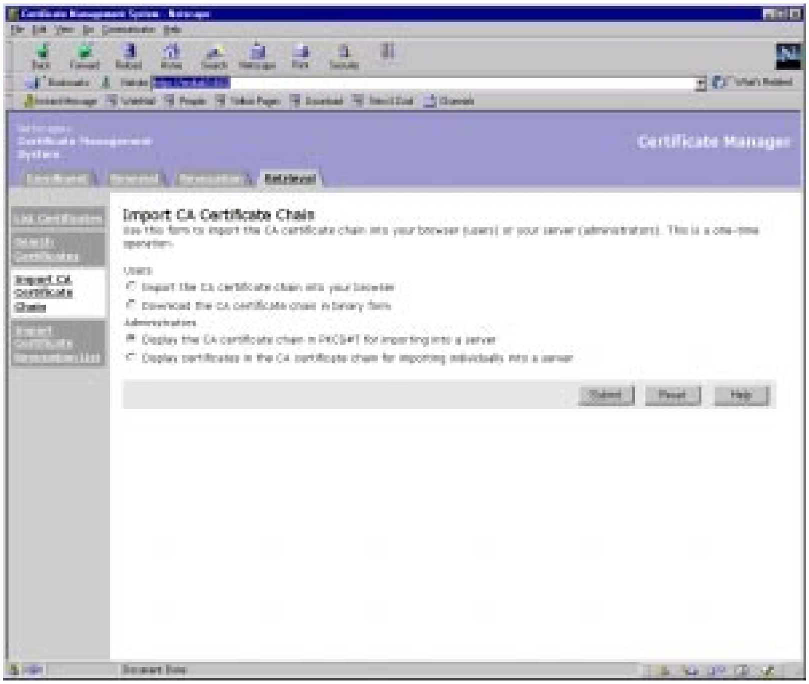
Phone:

Step 7 Click the **Retrieval** tab.

The retrieval page displays.

Step 8 Click **Import CA Certificate Chain**.

The Import CA Certificate Chain page displays.



Certificate Management System - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security
Bookmarks Netsite
What's Related
Netscape Certificate Management System
Certificate Manager
Enrollment Renewal Revocation Retrieval
List Certificates
Search Certificates
Import CA Certificate Chain
Import Certificate Revocation List
Submit Reset Help
Document: Done

Import CA Certificate Chain

Use this form to import the CA certificate chain into your browser (users) or your server (administrators). This is a one-time operation.

Users

○ Import the CA certificate chain into your browser

○ Download the CA certificate chain in binary form

Administrators

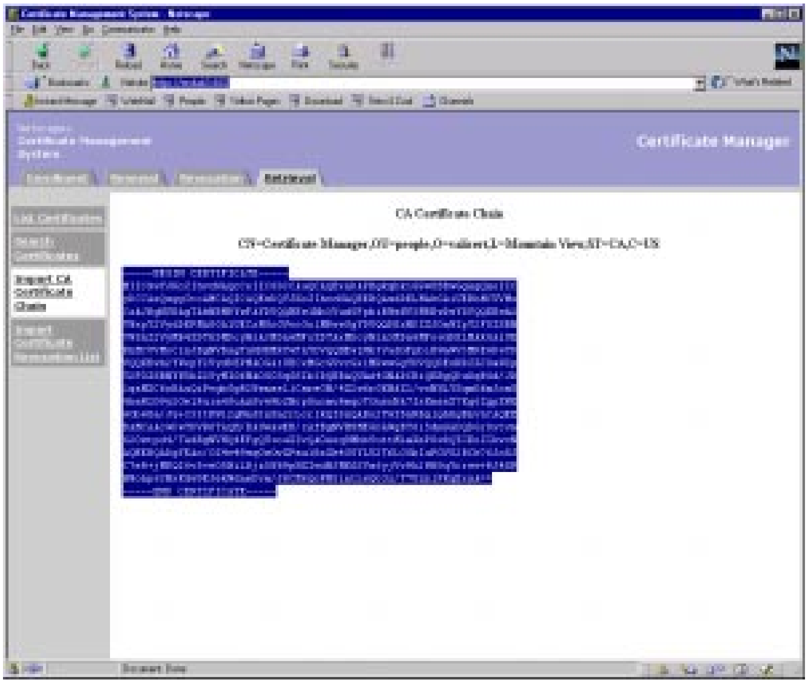
● Display the CA certificate chain in PKCS#7 for importing into a server

○ Display certificates in the CA certificate chain for importing individually into a server

Step 9 Select the **Display certificates in the CA certificate chain for importing individually into a server** radio button.

Step 10 Click **Submit**.

The CA Certificate Chain page displays:



Certificate Management System - Netscape
File Edit View Go Communicator Help
Back
Reload
Home
Search
Netscape
Print
Security
Bookmarks
Netsite
What's Related
Netscape Certificate Management System
Certificate Manager
Retrieval
List Certificates
Search Certificates
Import CA Certificate Chain
Import Certificate Revocation List
Document: Done

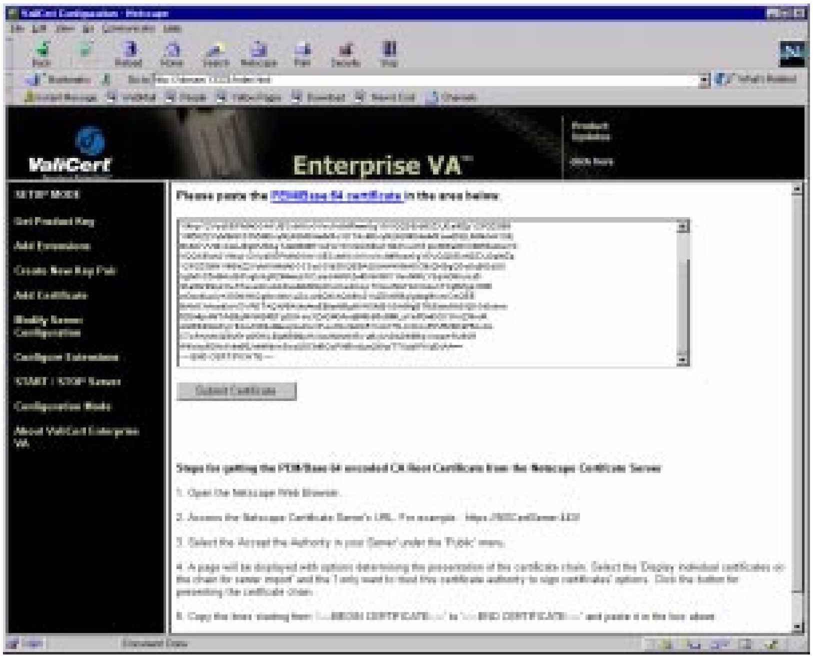
CA Certificate Chain

CN=Certificate Manager,OU=people,O=valicert,L=Mountain View,ST=CA,C=US

```
-----BEGIN CERTIFICATE-----
[illegible]
-----END CERTIFICATE-----
```

Step 11 Copy the certificate chain, including the `BEGIN CERTIFICATE` and `END CERTIFICATE` lines, to the clipboard.

Step 12 Paste the selection in the text area of the Add CA Root Certificate web page.



Please paste the PEM/Base 64 certificate in the area below:

```
-----END CERTIFICATE-----
```

Steps for getting the PEM/Base 64 encoded CA Root Certificate from the Netscape Certificate Server

1. Open the Netscape Web Browser.

2. Access the Netscape Certificate Server's URL. For example : https://NSCertServer:443/

3. Select the 'Accept the Authority in your Server' under the 'Public' menu.

4. A page will be displayed with options determining the presentation of the certificate chain. Select the 'Display individual certificates in the chain for server import' and the 'I only want to trust this certificate authority to sign certificates' options. Click the button for presenting the certificate chain.

5. Copy the lines starting from '-----BEGIN CERTIFICATE-----' to '-----END CERTIFICATE-----' and paste it in the box above.

Step 13 Click **Submit Certificate.**

The success web page displays.

Step 14 To continue with the configuration sequence click **Next Step**. The next step is Modifying the Enterprise VA Configuration.

Using the Microsoft Certificate Server 1.0 to Add Certificates

To add the CA root certificate using Microsoft Certificate Server 1.0

Step 1 If necessary click **Add Certificate** from the Setup menu.

Step 1 Click **Next Step** from the certificate information page if you are working in sequence, or click **Add Certificate** from the Setup menu.

The Add Certificate web page displays:

Step 2 Select the certificate format you want to use. To use Microsoft Certificate Server 1.0, select **DER encoded certificate (e.g. issued by Microsoft Certificate Server)**.

Step 3 Select the certificate store to which you want to add the certificate.

Certificate stores group certificates. The Administration Server provides a default set of stores in which you can place certificates. However, if you add an extension to the Enterprise VA, the stores can change.

By default, the Administration Server provides the following stores:

- Store that contains certificates of CAs publishing CRLs to the Enterprise VA
- Store that contains CA delegated certificates of the VA
- Store that contains certificates for signing OCSP/CRT responses
- Store that contains certificates for SLL communication with clients

If you have added any extensions to the Enterprise VA, such as the LDAP extension, OCSP extension, or your own extension, the Administration Server updates the list of available stores.

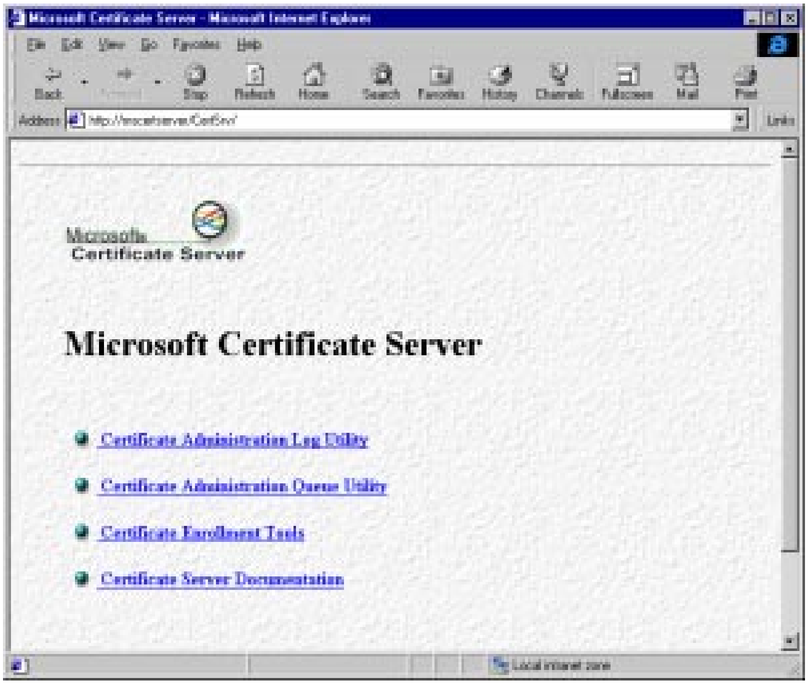
To add the root certificate, select **CA Certificate Stores Certificates of CAs publishing CRLs to the VA**.

Step 4 Click **Submit Certificate Type**.

Step 5 Open another browser window

Step 6 Enter the URL for the main Microsoft Certificate Server page, for example `http://MSCertServer/CertSrv`.

The Microsoft Certificate Server main page displays.



Microsoft Certificate Server - Microsoft Internet Explorer

Address: http://mscertserver/CertSrv/

Microsoft Certificate Server

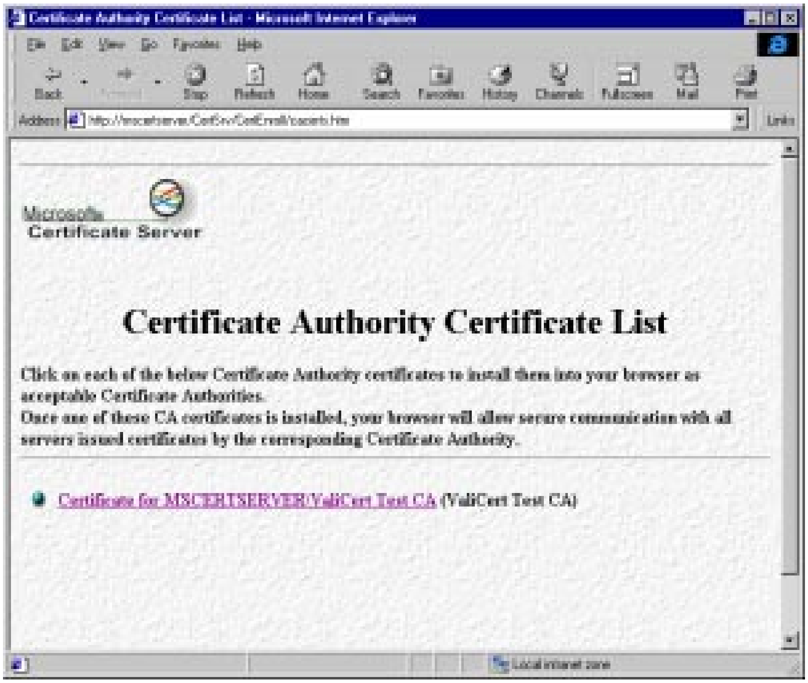
- Certificate Administration Log Utility
- Certificate Administration Queue Utility
- Certificate Enrollment Tools
- Certificate Server Documentation

Step 7 Click **Certificate Enrollment Tools**.

The Certificate Enrollment Tools page displays.

Step 8 Click **Install Certificate Authority Certificates**.

The Certificate Authority Certificate List page displays:



http://mscertserver/CertSrv/CertEnroll/cacerts.htm

Certificate Authority Certificate List

Click on each of the below Certificate Authority certificates to install them into your browser as acceptable Certificate Authorities.
Once one of these CA certificates is installed, your browser will allow secure communication with all servers issued certificates by the corresponding Certificate Authority.

- Certificate for MSCERTSERVER\ValiCert Test CA (ValiCert Test CA)

Step 9 Click the link corresponding to the CA certificate you need to load.

The File Download dialog box displays, asking whether you want to open the file or save it to disk.

Step 10 Select the **Save it to Disk** and click **OK**.

The Save As dialog box displays.

Step 11 Select the location where you want to save the file (which is named `<ca>.crt`). Note the location so you can specify it to the Enterprise VA. In this example, the file will be saved to the `c:\program files\valicert\entserv\mscerts` directory.

Step 12 Click **Save**.

The certificate is saved to the specified location.

Step 13 In the Administration server (the browser open to the ValiCert Enterprise VA configuration page), in the text field enter the complete path to the saved certificate.

Step 14 Click **Submit Certificate**.

The certificate is added to the Enterprise VA and the success web page displays.

NOTE: If you enter the path incorrectly, the error page displays. Click back and re-enter the complete path for the certificate.

Step 15 To continue with the configuration sequence click **Next Step**. The next step is Modifying the Enterprise VA Configuration.

Modifying the Enterprise VA Configuration

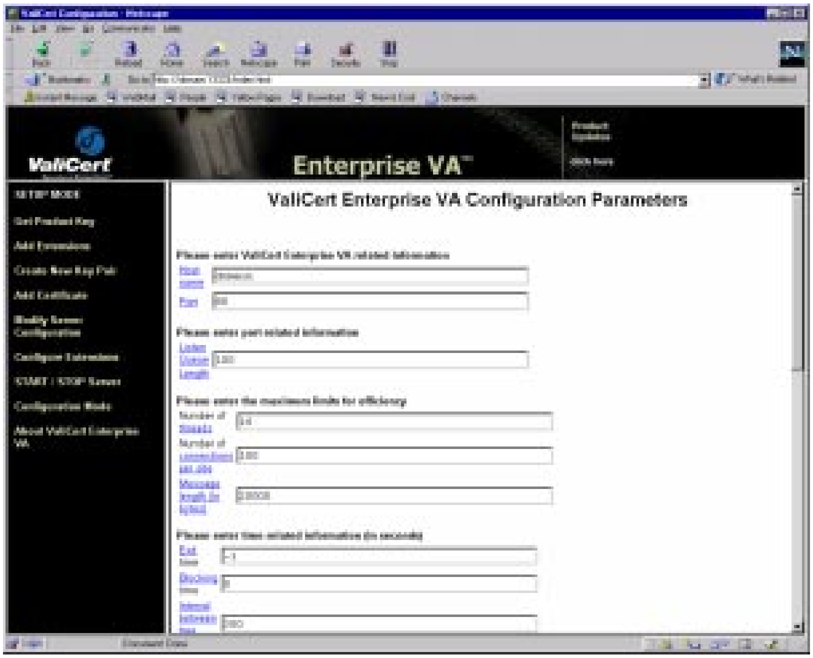
You can modify the Enterprise VA server configuration that was established during the installation process.

NOTE: When you install the ValiCert Enterprise VA, the default settings should be suitable for basic usage.

To modify the Enterprise VA configuration

Step 1 Click **Next Step** from the certificate added successfully page if you are working in sequence, or click **Modify Server Configuration** from the Setup menu.

The ValiCert Enterprise VA Configuration Parameters web page displays with the default settings that were established during installation:



ValiCert Enterprise VA Configuration Parameters

Please enter ValiCert Enterprise VA related information

Host name [illegible]

Port 80

Please enter port related information

Listen Queue Length 100

Please enter the maximum limits for efficiency

Number of threads 64

Number of connections per job 100

Message length in bytes 10000

Please enter time related information (in seconds)

Exit time -1

Blocking time 0

Internal Refresh time 3600

Step 2 Modify the information on this page.

Table 3 lists and briefly describes the configuration parameters that you can specify at this web page and their ves section equivalents.

NOTE: These parameters are contained within the `[ves]` section of the `valicert.ini` file.

Table 3. Setup Configuration Parameters

Setup Parameter	ves Section Parameter	Description
Host name	`serverHost`	Name of your machine (it should NOT be set to `localhost`).
Port	`serverHost`	Port on which ValiCert Enterprise VA runs (Default: 80).

Table 3. Setup Configuration Parameters (Continued)

Setup Parameter	ves Section Parameter	Description
Listen Queue Length	`listenLength`	Number of requests that can be contained in the listen queue. The default is 100 requests.
Number of threads	`maxThread`	Number of pre-spawned threads Enterprise VA uses to process jobs. More threads enable you to support more clients in parallel, but require more system resources to run the Enterprise VA.
Number of connections per site	`maxConnPerSite`	Number of simultaneous connections a single machine can make to the ValiCert Enterprise VA.
Message length (in bytes)	`maxMsgLen`	Maximum message size of any message. Prevents attacks where the server is maliciously sent large amounts of irrelevant data.
Exit time	`exitTime`	Optional time (in seconds) in which the server will automatically stop and restart.
Blocking time	`blockTime`	Time the server will wait for a message to get through. Prevents attacks where someone sends you data and then stops.
Interval between tree updates	`nextUpdatePeriod`	Time between tree production. A lower value will cause more trees to be produced. The maximum frequency is dictated by your license type.
Log file directory and prefix	`logFile`	Prefix append to log files and the log folder in the form `<logdir>/<prefix>`, for example `log/va`. Log files are created with the prefix and a time stamp appended to them and they are stored in the specified directory. If you specify a directory other than the default, you must create the directory.
Local Build	`buildLocal`	Must be set to `1`, specifying that the ValiCert Enterprise VA builds CRTs from local CRLs.

Table 3. Setup Configuration Parameters (Continued)

Setup Parameter	ves Section Parameter	Description
Mechanism for signing OCSP Responses	`useSoftwaresigning`	Software: Sign using BSAFE is the default. Hardware: Sign using hardware token.
SSL Signing Type	`sslSigningType`	Software: Sign using BSAFE is the default. Hardware: Sign using hardware token.
‘Servername: Port’ of SSL connections	`sslServerHost`	Servername:port on which Enterprise VA listens for SSL connections.
SSL Server’s site certificate	`sslCertFile`	Filename containing the local SSL server’s site certificate in base64 format, including `---Begin Certificate---` and `---End Certificate---` lines.
SSL Server’s Private Key File	`sslPrivateKey`	Filename containing the local SSL server’s encrypted private key encoded in base64 format
Time in sec. for which to use a CRL after it expires	`useExpiredCRLs`	Determines the number of seconds a CRL can be used after it is expired. If CRL is expired, clients will receive an ‘Unknown CA’ error.
Time in sec. for which OCSP responses are valid	`maxOCSPValidityPeriod`	Variable to specify whether or not to include a validity period in outgoing OCSP responses; 0: do not include the next update period in the response positive number ‘n’: OCSP response valid for the lesser of n seconds or the validity period specified in the original CRL negative number: use validity period as defined by associated CRL.

Step 3 Click **Submit Configuration Parameters** to apply the changes.

The configuration updated success web page displays.

Step 4 To proceed with the next step for first time configuration click **Next Step**. The next step is Configuring Extensions.

Step 5 If you have not added any extensions, you are given the option to either add extensions, (click on **Add Extensions**) or to skip this step, (click on **Next**).

Configuring and Deleting Extensions

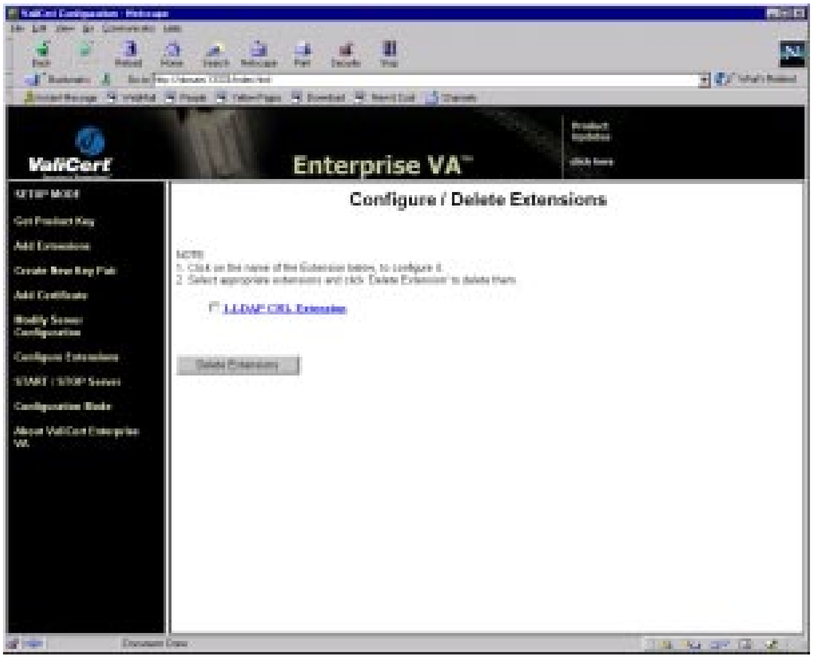
You can configure or remove any extensions that you added earlier. Extensions are added using the Add Extensions option from the Setup menu. Extensions are configured or deleted from the Configure/Delete Extensions web page.

Only extensions which have been added are listed.

To display the Configure/Delete Extensions web page

Step 1 Click **Next Step** from the Configuration Updated Successfully page if you are working in sequence, or click **Configure Extensions** from the Setup menu.

The Configure/Delete Extensions web page displays:



Configure / Delete Extensions

NOTE:
1. Click on the name of the Extension below, to configure it.
2. Select appropriate extensions and click 'Delete Extension' to delete them.

□ 1.LDAP CRL Extension

Delete Extensions

To delete extensions

Step 1 Select any extensions to delete.

Step 2 Click **Delete Extensions**.

The selected extensions are removed.

To configure or delete extensions

Step 3 Click on the name of the extension you are configuring.

A web page for that extension displays.

Step 4 Follow the on-screen instructions for the extension.

Step 5 Click **Submit Extension Configuration Changes**.

The Extension Configuration Success web page displays.

Step 6 To proceed with the next step for first time configuration click **Next Step**. The next step is and Stopping the Enterprise VA Server on Windows NT.

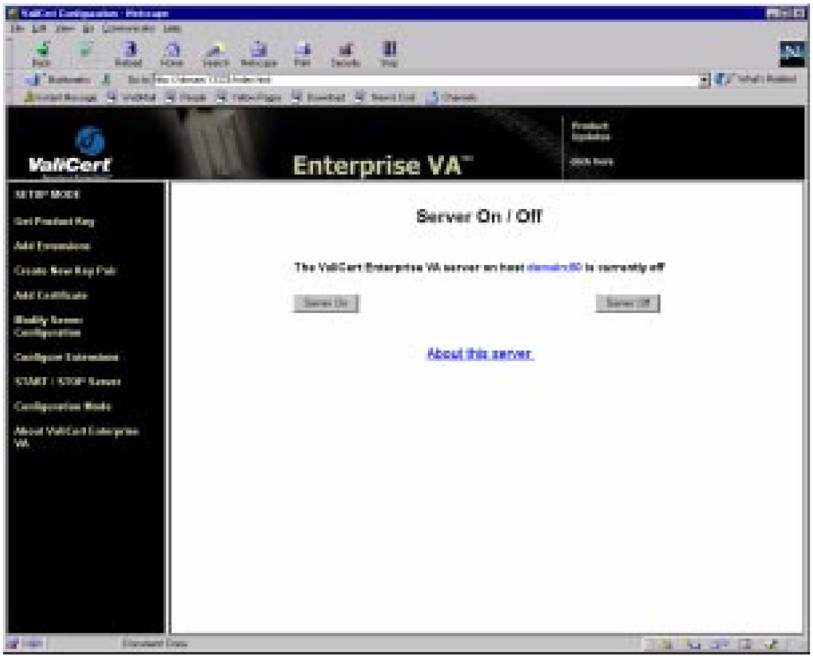
Starting and Stopping the Enterprise VA Server on Windows NT

You can start and stop the Enterprise VA server on Windows NT from the Server On/Off page.

To start or stop the Enterprise VA server host on Windows NT

Step 1 Click **Next Step** from the extension configuration updated successfully page if you are working in sequence, or click **Start/Stop Server** from the Setup menu.

The Server On/Off web page displays:



Server On / Off

The ValiCert Enterprise VA server on host domain:80 is currently off

Step 2 Click **Server On** or **Server Off**.

Any time you start the server, you will need to enter the server password (at the console) specified during configuration of the Enterprise VA.

NOTE: Because the password must be entered at the console, remote starting of the server may not be possible.

Your ValiCert Enterprise VA is now active. You can browse the logs and administer the server.

NOTE: When the server status changes, you must click the Reload/Refresh button on your browser to view the current server status.

If you stop the Enterprise VA, the Enterprise VA becomes inactive, but you can continue to use the Administration Server interface.

Starting and Stopping the Enterprise VA Server on UNIX

You need to use the `vactl` script to start, stop, or restart the Enterprise VA. This script is located in the `<VAInstallDir>/va/entserv` directory.

To start the Enterprise VA

❖ Type the following at the command prompt:

```
vactl start
```

You are now ready to use the Management Menu.

Proceed to Chapter 4, "Working at the Configuration Mode Menu."

NOTE: When you start the Enterprise VA, you must manually refresh your browser to see the new status.

To stop the Enterprise VA

❖ Type the following at the command prompt:

```
vactl stop
```

To restart the ValiCert Enterprise VA

❖ Type the following at the command prompt:

```
vactl restart
```

NOTE: When you reboot your machine, the ValiCert Enterprise VA (as a part of the startup) will require you to enter the administrative password.

CHAPTER
4

Working at the Configuration Mode Menu

This section describes the various management and configuration tasks that you can perform at the Enterprise VA administration server from the Configuration Mode menu.

- Manage keys and certificates
- Manage the Enterprise VA server
- Manage certificate stores
- Manage extensions
- View logs
- Configure other ValiCert products

To access the Configuration Mode menu, if necessary click **Configuration Mode** on the left hand side of the administration screen.

If you are in Configuration Mode, to go to Setup mode, click **Back to SETUP**.

Managing Keys and Certificates

This section describes how to manage keys and certificates from the Configuration Mode menu. To access the pages for managing keys and certificates, in the Configuration Mode menu, click **Manage Keys and Certificates**. Menu options that correspond to the following tasks display:

- Getting New Product Key
- Generating a New Private Key
- Viewing the VA Certificate

- ❖ Downloading the VA Certificate
- ❖ Displaying Certificate Requests

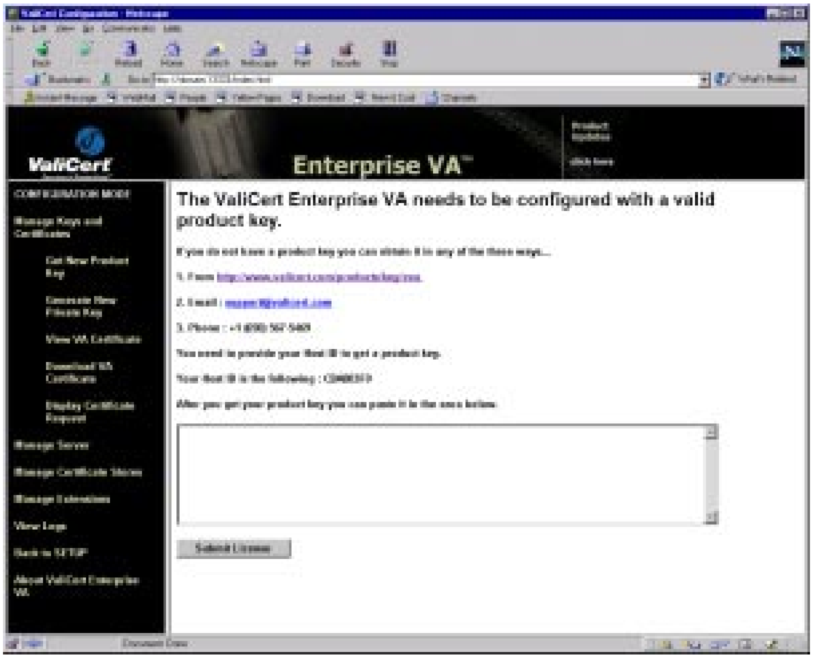
Getting New Product Key

You must have a product key to use the Enterprise VA. You have already created one during setup. If for any reason you wish to get a new product key, you can do so at the Configuration Mode menu.

To get a new product key

Step 1 Click **Get New Product Key** in the Configuration Mode menu.

The product key page displays.



The ValiCert Enterprise VA needs to be configured with a valid product key.

If you do not have a product key you can obtain it in any of the three ways...

1. From http://www.valicert.com/products/key/eva.

2. Email : support@valicert.com

3. Phone : +1 (650) 567 5469

You need to provide your Host ID to get a product key.

Your Host ID is the following : [illegible]

After you get your product key you can paste it in the area below.

Step 2 Get the product key by one of the following methods:

a Note your `hostid` and click `http://www.valicert.com/products/key/eva`. The ValiCert Product Evaluation Key Center page displays. On this page, enter the requested information, including your `hostid` from the previous page. Select whether you want to be on the ValiCert mailing list and click **Submit Request**.

A page displaying your product key opens. Copy the license information to the Clipboard.

b Send e-mail to `support@valicert.com`. Be sure to include your `hostid` in the body of the message.

c Call ValiCert at the number listed on the page. Be sure you have your `hostid` available when you call.

Step 3 Paste the license information into the product key area of ValiCert Product Evaluation Key Center page.

Step 4 Click **Submit License**.

The web page indicting that the product key has been updated successfully displays.

Generating a New Private Key

When you generate a new private key (and the associated public key), you have the option to backup or overwrite the existing key.

- A new certificate signing request is generated. You can also generate a self-signed certificate.
- Passwords for all private keys must be the same
- You can use hardware or software to generate the key pairs.

For instructions on creating key pairs with software see “Creating Key Pairs” on page 51 or for instructions on creating key pairs with hardware, see “Generating Hardware Keys” on page 150.

Viewing the VA Certificate

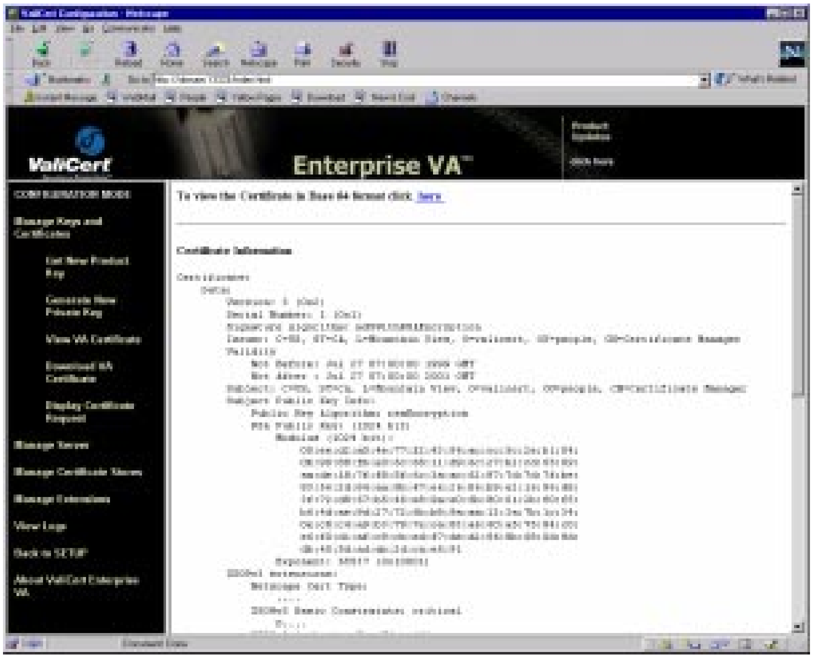
The ValiCert Enterprise VA certificate is used to sign validation responses. This is either a self-signed or delegated certificate which contains the information entered when the certificate request was generated.

When a client application user views a validation response that is signed by the ValiCert Enterprise VA, the user sees the information that you entered when you generated your key pair.

To view the ValiCert Enterprise VA certificate:

Step 1 Under the Manage Keys and Certificates section of the Configuration Mode menu, click **View VA Certificate**.

The key type web page displays with the data component of the certificate, and the base-64 encoded representation of the certificate.



To view the Certificate in Base 64 format click here

Certificate Information

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=US, ST=CA, L=Mountain View, O=valicert, OU=people, CN=Certificate Manager
        Validity
            Not Before: Jul 27 07:00:00 2000 GMT
            Not After : Jul 27 07:00:00 2001 GMT
        Subject: C=US, ST=CA, L=Mountain View, O=valicert, OU=people, CN=Certificate Manager
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    [illegible]
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            Netscape Cert Type:
                ....
            X509v3 Basic Constraints: critical
                C:...
```

Downloading the VA Certificate

You can download a base-64 encoded version of your ValiCert Enterprise VA certificate to a file. This is useful if you want to send the certificate to a client application that needs to add the Enterprise VA root certificate.

To download the VA certificate

Step 1 Under the Manage Keys and Certificates section of the Configuration Mode menu, click **Download VA Certificate**.

The File Download dialog box displays.

Step 2 Select **Save this file to disk** and click **OK**.

The Save As dialog box displays.

Step 3 Enter a file name for the certificate and select the location to store the certificate file.

Step 4 Click **Save**.

The certificate is saved.

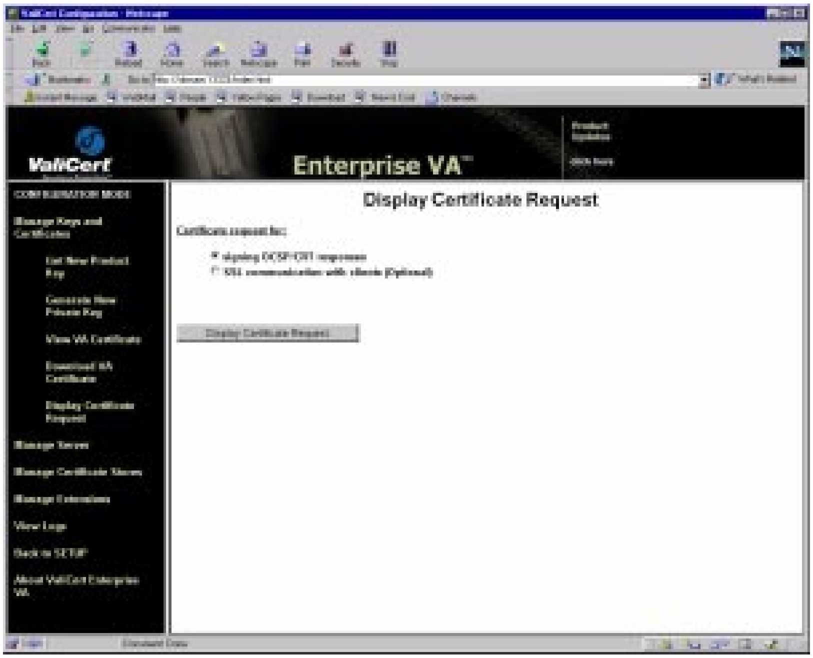
Displaying Certificate Requests

You can view any of the certificate requests that have been created with the Enterprise VA.

To display a certificate request

Step 1 Under the Manage Keys and Certificates section of the Configuration Mode menu, click **Display Certificate Request**.

The Display Certificate Request web page displays.



Certificate request for:

● signing OCSP-CRT responses
○ SSL communication with clients (Optional)

Step 2 Select the certificate request to display and click **Display Certificate Request**.

The selected certificate request displays.

Managing the Server

This section describes how to configure, start and stop the Enterprise VA server from the Configuration Mode menu. To access the pages for managing the server, in the Configuration Mode menu, click **Manage Server**. Menu options that correspond to the following tasks display:

- ❖ Configuring the Enterprise VA Server
- ❖ Starting and Stopping the Enterprise VA Server on NT
- ❖ Mirroring ValiCert Global VA Service Data

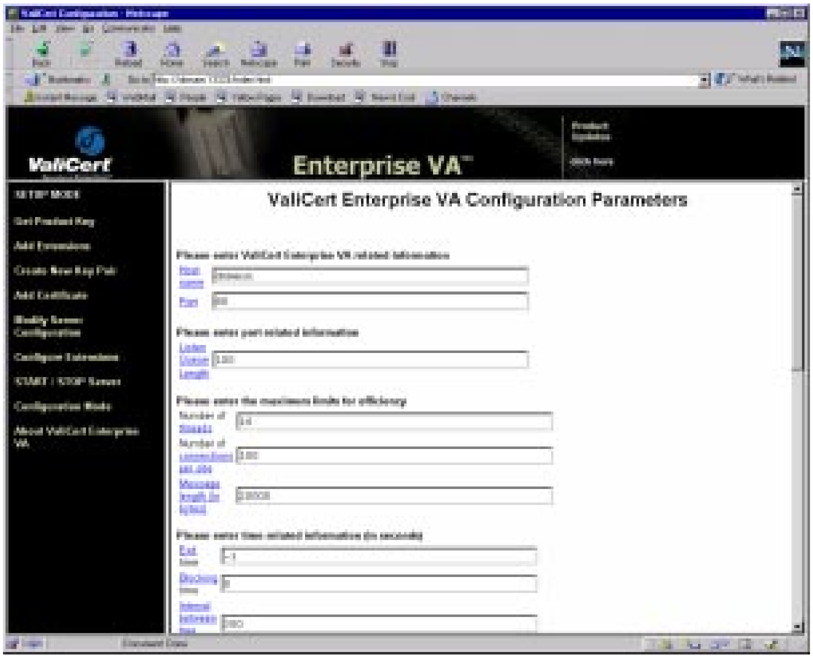
Configuring the Enterprise VA Server

You can dynamically modify the configuration of the Enterprise VA file from the Administration Server interface.

To modify the Enterprise VA configuration

Step 1 Under the Manage Server section of the Configuration Mode menu, click **Configure Server**.

The ValiCert Enterprise VA Configuration Parameters web page displays with the current server settings.



ValiCert Enterprise VA Configuration Parameters

Please enter ValiCert Enterprise VA related information

Host name

Port

Please enter port related information

Listen Queue Length

Please enter the maximum limits for efficiency

Number of threads

Number of connections per one

Message length (in bytes)

Please enter time related information (in seconds)

Exit time -1

Blocking time 0

Interval between

Step 2 Modify the information on this page.

See “Modifying the Enterprise VA Configuration” on page 67 for detailed descriptions of the configuration parameters.

Step 3 Click **Submit Configuration Parameters** to apply the changes.

The configuration updated success web page displays.

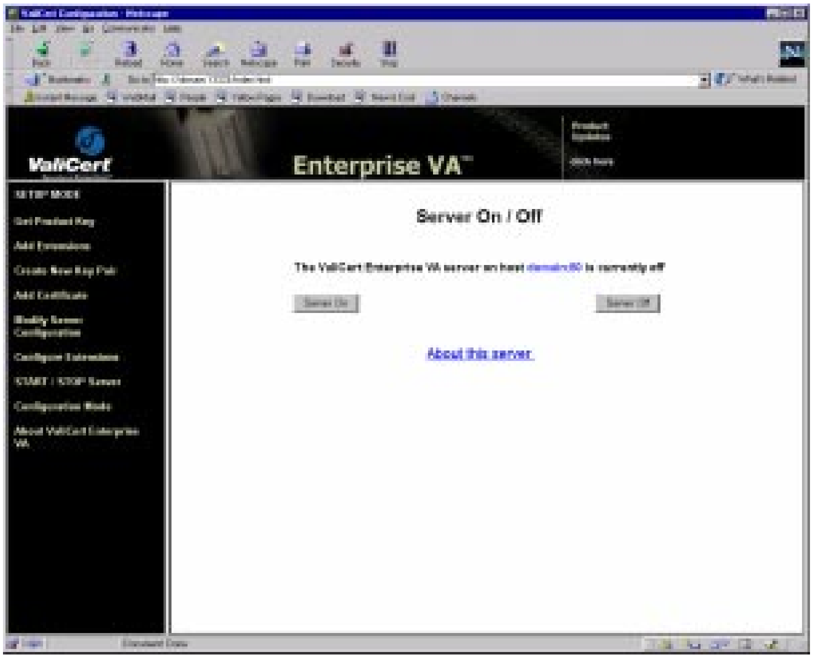
Starting and Stopping the Enterprise VA Server on NT

You can start and stop the Enterprise VA server that is running on Windows NT, from the Configuration Mode menu.

To start or stop the Enterprise VA server host on Windows NT

Step 1 Under the Manage Server section of the Configuration Mode menu, click **Start/Stop Server**.

The Server On/Off web page displays with the current server settings:



Server On / Off

The ValiCert Enterprise VA server on host domain:80 is currently off

Step 2 Click **Server On** or **Server Off**.

NOTE: When the server status changes, click the Reload/Refresh button on your browser to view the current server status.

To start the server, you must enter the server password (at the console). This is the password for the keys, specified when the ValiCert Enterprise VA was configured.

NOTE: Because the password must be entered at the console, remote starting of the server may not be possible.

Your ValiCert Enterprise VA is now active. You can browse the logs and administer the server.

For instructions on starting and stopping a UNIX server, see “Starting and Stopping the Enterprise VA Server on UNIX” on page 74

Mirroring ValiCert Global VA Service Data

The Mirroring Global VA Service mirrors data from ValiCert’s Global VA Service. The Global VA Service is a trusted third party validation solution that provides you with access to a global network of certificate and application specific validation information.

The mirroring feature allows your Enterprise VA to locally cache Global VA Service validation data from one or more public CAs. Locally cached data enables the Enterprise VA to provide validation data to its users without requiring numerous, separate requests to the Global VA Service. Instead, the Enterprise VA can rely on its own locally cached data to respond to the validation requests from users within the enterprise thus, improving validation performance.

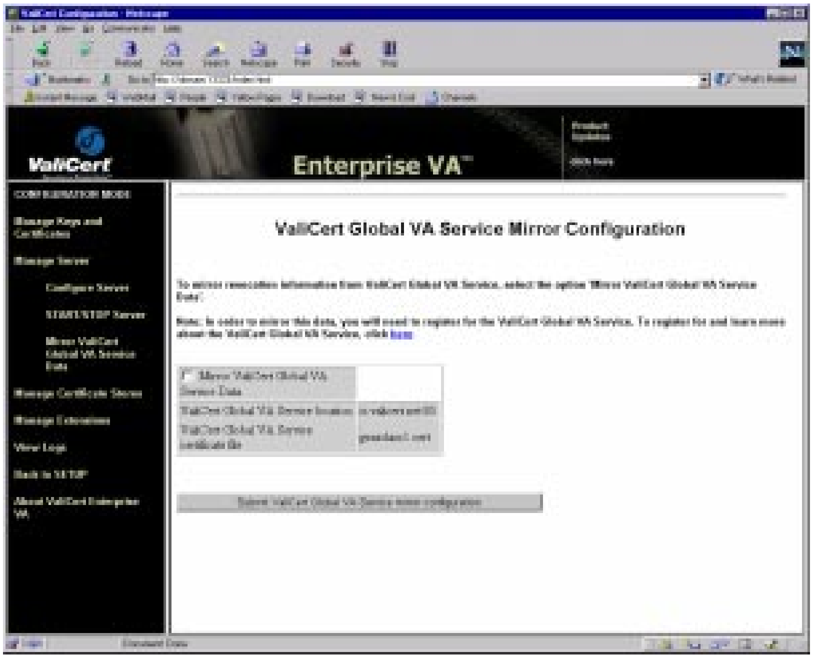
When the Global VA Service receives CRLs from public CAs, it builds CRTs. It can then send all the CRTs to your Enterprise VA to be cached locally. The Global VA Service updates these CRTs periodically as they expire. CRTs expire in accordance with the expiration time set by the Global VA Service component that builds the CRT.

NOTE: In order to mirror this data, you will need to register for the ValiCert Global VA Service. For more information see http://www.valicert.com/html/gvas.html.

To mirror Global VA Service data

Step 1 Under the Manage Server section of the Configuration Mode menu, click **Mirror ValiCert Global VA Service Data**.

The ValiCert Global VA Service Mirror Configuration web page displays with the current Global VA Service settings:


ValiCert Configuration - Netscape
ValiCert
Enterprise VA™
Product Updates
CONFIGURATION MODE
Manage Keys and Certificates
Manage Server
Configure Server
START/STOP Server
Mirror ValiCert Global VA Service Data
Manage Certificate Stores
Manage Extensions
View Logs
Back to SETUP
About ValiCert Enterprise VA
Submit ValiCert Global VA Service mirror configuration

ValiCert Global VA Service Mirror Configuration

To mirror revocation information from ValiCert Global VA Service, select the option 'Mirror ValiCert Global VA Service Data'.

Note: In order to mirror this data, you will need to register for the ValiCert Global VA Service. To register for and learn more about the ValiCert Global VA Service, click here

☐ Mirror ValiCert Global VA Service Data	
ValiCert Global VA Service location	[illegible]
ValiCert Global VA Service certificate file	[illegible]

Step 2 Click **Mirror ValiCert Global VA Service Data** to enable mirroring.

NOTE: The availability of Global VA Service mirroring mode is dependent on your license.

The ValiCert Global VA Service location and certificate file can be viewed but not modified from this administrative interface. These values correspond to the `masterHosts` and `vgvsCertFile` parameters defined in the `valicert.ini` file.

Step 3 Click **Submit ValiCert Global VA Service** mirror configuration.

The success dialog box displays.

Step 4 Restart the server for the change to take effect.

Managing Certificate Stores

This section describes how to manage certificate stores from the Configuration Mode menu. To access the pages for certificate stores, in the Configuration Mode menu, click **Manage Certificate Stores**. Menu options that correspond to the following tasks display:

- Adding Certificates to a Store
- Viewing and Modifying Certificate Stores

Certificate stores group certificates. The Administration Server provides a default set of stores in which you can place certificates. However, if you add an extension to the Enterprise VA, such as the LDAP extension, OCSP extension, or your own extension, more stores can be added.

By default, the Administration Server provides the following stores:

- Store that contains certificates of CAs publishing CRLs to the Enterprise VA
- Store that contains CA delegated certificates of the VA
- Store that contains certificates for signing OCSP/CRT responses
- Store that contains certificates for SLL communication with clients

Adding Certificates to a Store

You can add certificates to any of the stores known to the Enterprise VA. The stores available depend on the extensions you have added.

Preparing the Certificate

The way that you submit the certificate depends on the format of the certificate. The format is either DER encoded or Base 64 encoded (PEM).

To prepare DER encoded certificates:

Step 1 Obtain the certificate

Step 2 Copy (or download) the certificate to a known location for example `C:\Program Files\ValiCert\EnterpriseVA\mscerts\`.

To prepare Base 64 encoded (PEM) certificates

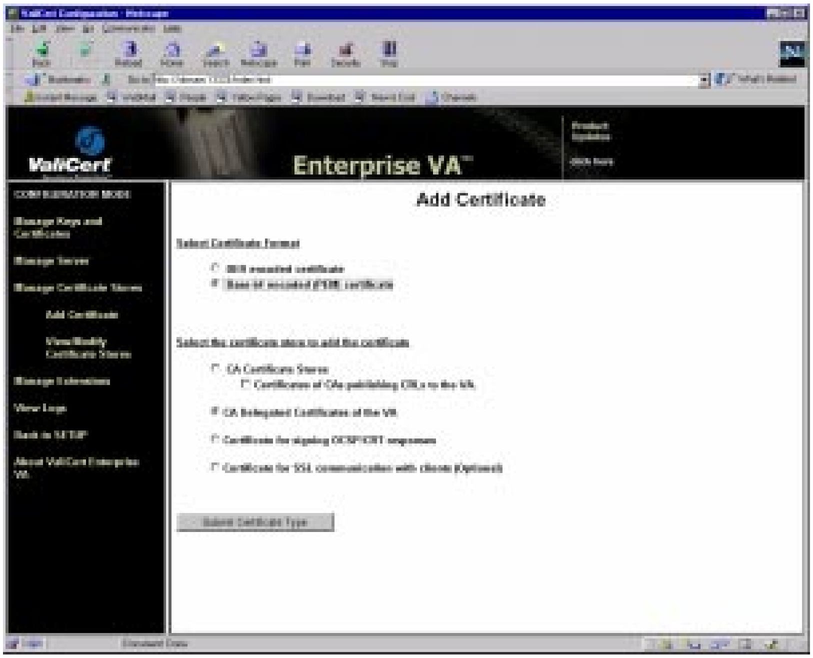
Step 1 Display the certificate in a text editor or browser window.

Step 2 Copy the text of the certificate to your clipboard. Make sure you copy the entire certificate including the lines that contain `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----`.

To add a certificate to a certificate store

Step 1 Under the Manage Certificate Stores section of the Configuration Mode menu, click **Add Certificate**.

The Add Certificate web page displays:



Add Certificate

Select Certificate Format

○ DER encoded certificate

● Base 64 encoded (PEM) certificate

Select the certificate store to add the certificate

☐ CA Certificate Stores

☐ Certificates of CAs publishing CRLs to the VA

☑ CA Delegated Certificates of the VA

☐ Certificate for signing OCSP/CRT responses

☐ Certificate for SSL communication with clients (Optional)

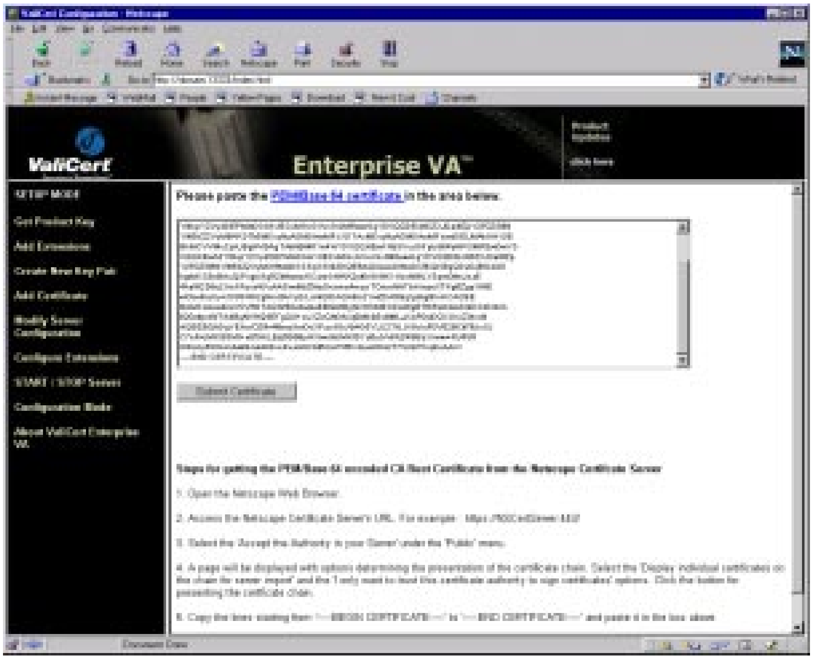
Step 2 Select the certificate format of the certificate you want to add.

Step 3 Select the certificate store to which you want to add the certificate.

Step 4 Click **Submit Certificate**.

NOTE: The way that you submit the certificate depends on which type of certificate you are importing, DER or Base64.

For **Base 64 encoded certificates** the submit Base 64 certificate screen displays:



Please paste the PEM/Base 64 certificate in the area below.

Steps for getting the PEM/Base 64 encoded CA Root Certificate from the Netscape Certificate Server

1. Open the Netscape Web Browser.

2. Access the Netscape Certificate Server's URL. For example: https://NSCertServer:443/

3. Select the 'Accept this Authority in your Server' under the 'Public' menu.

4. A page will be displayed with options determining the presentation of the certificate chain. Select the 'Display individual certificates in the chain for server import' and the 'I only want to trust this certificate authority to sign certificates' options. Click the button for presenting the certificate chain.

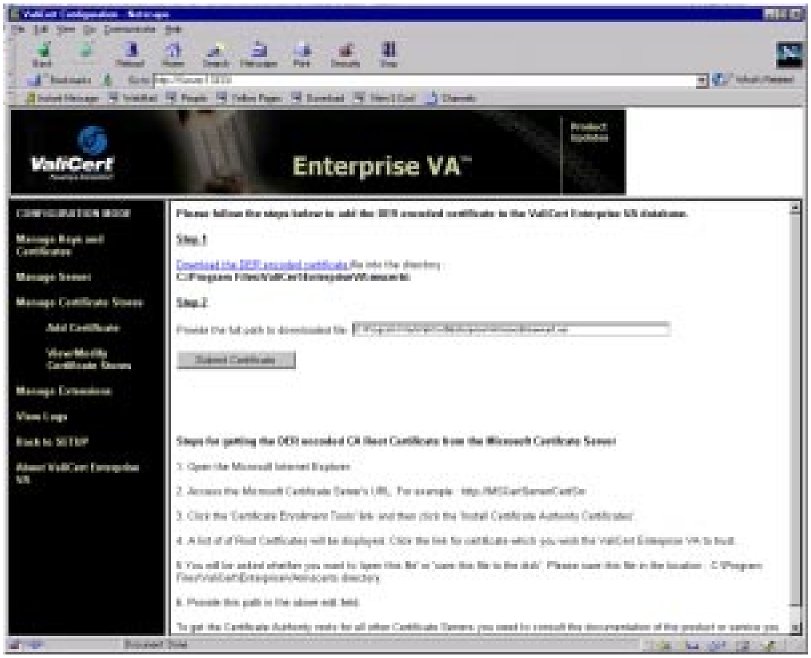
5. Copy the lines starting from '-----BEGIN CERTIFICATE-----' to '-----END CERTIFICATE-----' and paste it in the box above.

Step 5 Paste the certificate in the text area of the web page.

Step 6 Click **Submit Certificate**.

The success web page displays.

For **DER encoded Certificates** the submit DER certificate screen displays:



Please follow the steps below to add the DER encoded certificate to the ValiCert Enterprise VA database.

Step 1

Download the DER encoded certificate file into the directory : C:\Program Files\ValiCert\Enterprise\VA\[illegible]

Step 2

Provide the full path to downloaded file: [illegible]

Steps for getting the DER encoded CA Root Certificate from the Microsoft Certificate Server

1. Open the Microsoft Internet Explorer

2. Access the Microsoft Certificate Server's URL. For example : http://MSCertServer/CertSrv

3. Click the 'Certificate Enrollment Tools' link and then click the 'Install Certificate Authority Certificates'

4. A list of all Root Certificates will be displayed. Click the link for certificate which you want the ValiCert Enterprise VA to trust.

5. You will be asked whether you want to 'open this file' or 'save this file to the disk'. Please save this file in the location : C:\Program Files\ValiCert\Enterprise\VA\[illegible] directory.

6. Provide this path in the above edit field.

To get the Certificate Authority roots for all other Certificate Servers you need to consult the documentation of the product or service you

Step 5 Enter the full path to the certificate in the **Provide the full path to downloaded file** field.

Step 6 Click **Submit Certificate**.

The success web page displays.

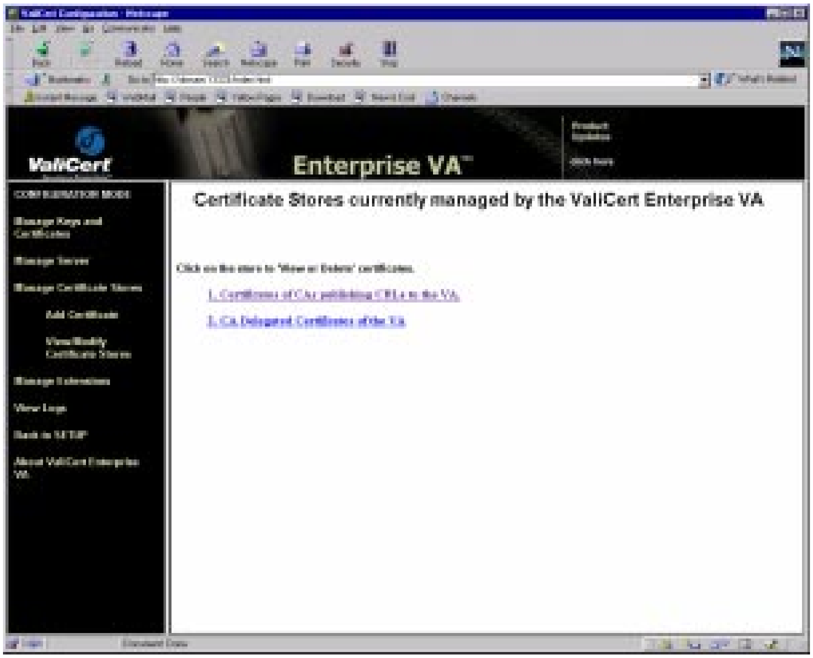
Viewing and Modifying Certificate Stores

You can view or delete the certificates in the various certificate stores.

To view or delete certificates from a store

Step 1 Under the Manage Certificate Stores section of the Configuration Mode menu, click **View/Modify Certificate Stores**.

The Certificate Stores web page displays with the list certificate stores managed by the Enterprise VA:



Certificate Stores currently managed by the ValiCert Enterprise VA

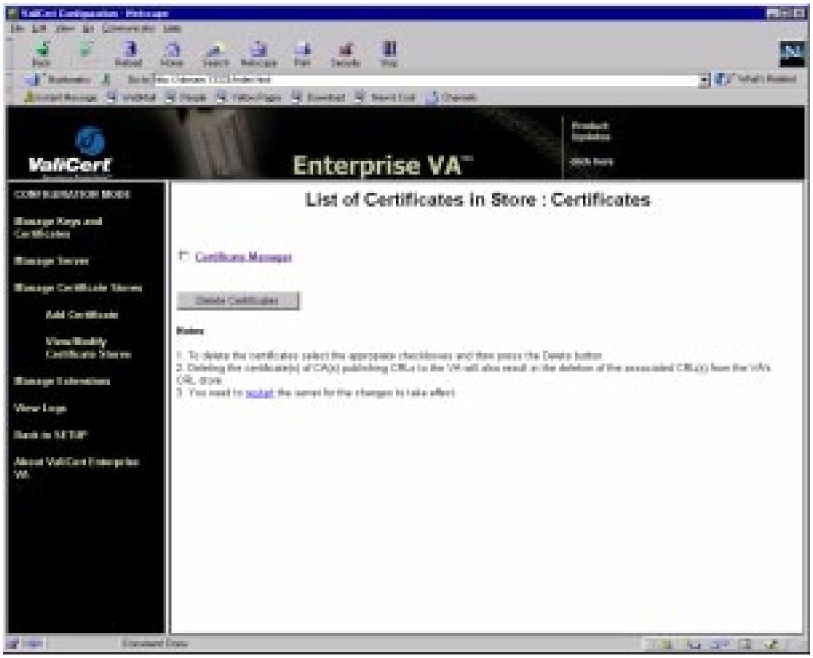
Click on the store to 'View or Delete' certificates.

1. Certificates of CAs publishing CRLs to the VA.

2. CA Delegated Certificates of the VA

Step 2 Select a store.

The List of Certificates web page displays with the list of certificates in the store:


ValiCert Configuration - Netscape
ValiCert
Enterprise VA™
Product Updates
click here
CONFIGURATION MODE
Manage Keys and Certificates
Manage Server
Manage Certificate Stores
Add Certificate
View/Modify Certificate Stores
Manage Extensions
View Logs
Back to SETUP
About ValiCert Enterprise VA

List of Certificates In Store : Certificates

☐ Certificate Manager

Delete Certificates

Notes

1. To delete the certificates select the appropriate checkboxes and then press the Delete button
2. Deleting the certificate(s) of CA(s) publishing CRLs to the VA will also result in the deletion of the associated CRL(s) from the VA's CRL store
3. You need to restart the server for the changes to take effect

Step 3 Click a certificate's link to view it.

Step 4 To delete a certificate, select its checkbox.

(You can delete multiple certificates at one time.)

Click **Delete Certificates** to delete the certificate.

NOTE: You may need to restart the server for the deletion to take effect.

Managing Extensions

This section describes how to manage extensions from the Configuration Mode menu. To access the pages for extensions, in the Configuration Mode menu, click **Manage Extensions**. Menu options that correspond to the following tasks display:

- Adding Extensions
- Configuring/Deleting Extensions

Adding Extensions

The Enterprise VA Administration Server interface by default allows you to add the LDAP and OCSP ValiCert extensions. Add any extensions you have created the Extension API, through this interface.

NOTE: To add and manage your own extension through the Administration Server the appropriate files must be place in the `entserv` directory.

For Windows NT, the extensions's `.ecf` file and `.dll` must be located in the following directory:

```
<VAInstallDir>\EnterpriseVa\entserv\
```

For UNIX, the extensions's `.ecf` file and `.so` must be located in the following directory:

```
<VAInstallDir>/va/entserv/
```

To add an extension

Step 1 Click **Add Extensions** from the Configuration Mode menu.

The Add Extensions web page displays.

Step 2 Select any extensions you want to add.

You can add one or more extensions at a time.

Step 3 Click **Add Extension**.

The extensions added successfully web page displays. On this page there are links to other configuration pages.

Step 4 Click the link to add more Extensions.

OR

Click the link to configure the newly added extension.

OR

Click **restart** to go to the Server On/Off page to restart the server to activate the extension.

Configuring/Deleting Extensions

You can configure each of the extensions you have added. The order in which you configure the extensions determines the order in which their extension section is added to the `valicert.ini` file. This in turn, determines the order in which extension processing occurs if more than one extension is requested at the same stage. For details about staged request processing by the Enterprise VA, see Chapter 5, "Writing a VA Extension."

For details about configuring or deleting an extension, see “Configuring and Deleting Extensions” on page 71

NOTE: You need to restart the server for the configuration or deletion to take effect.

Viewing Logs

You can view log files that the Enterprise VA maintains about activity taking place on the server.

The Enterprise VA supports the following logs:

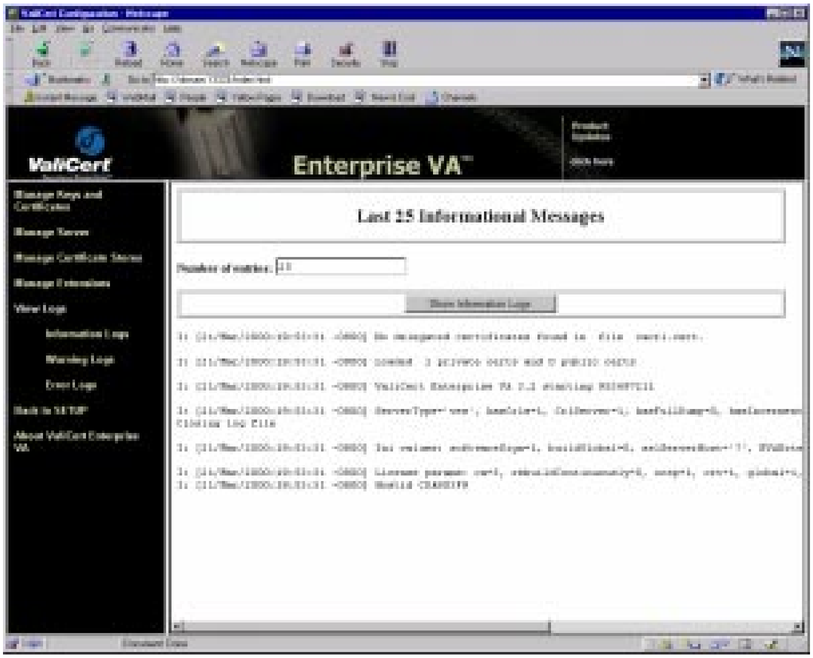
- Information logs—contains information about validation requests processed by the Enterprise VA.
- Warning logs—contain warning messages issued by the Enterprise VA.
- Error logs—contain error messages issued by the Enterprise VA.

For a description of possible log messages, see
Appendix F, "Troubleshooting"

To view a log

- Select the log you want to view from the Configuration Mode menu.

A web page with the selected log displays. The following is an example of the Information log:



Last 25 Informational Messages

Number of entries: 25

```
I: [21/Mar/2000:20:51:31 -0800] No unexpired certificates found in  file  [illegible]
I: [21/Mar/2000:20:51:31 -0800] Loaded  2 private certs and 0 public certs
I: [21/Mar/2000:20:51:31 -0800] ValiCert Enterprise VA 2.2 starting [illegible]
I: [21/Mar/2000:20:51:31 -0800] ServerType='[illegible]', [illegible]
Closing Log File
I: [21/Mar/2000:20:51:31 -0800] Ini values: [illegible]
I: [21/Mar/2000:20:51:31 -0800] License params: [illegible]
I: [21/Mar/2000:20:51:31 -0800] Build [illegible]
```

Creating a New Log File Directory and Files

If you attempt to view a log and get the message "Unable to open log files. Please check the ValiCert VA configuration" it is because the log file directory specified in the configuration does not exist. You must manually create the directory specified in the Configure Server page or change it to an existing file. For more information see “Modifying the Enterprise VA Configuration” on page 67.

CHAPTER 5

Writing a VA Extension

This section provides information to help you write an extension that extends the functionality of the Enterprise VA to include Stateful Validation™ that is, application-specific or context-specific processing tailored to your requirements.

NOTE: You can implement an Enterprise VA extension either as a DLL (on Windows NT) or a shared object (on UNIX).

The VA API provides the mechanism by which an extension can seamlessly integrate into the Enterprise VA validation cycle and alter the request processing flow to include processing that is to be done by the extension application.

To understand the role of an extension, it is important to understand how the Enterprise VA processes requests.

The Enterprise VA performs its request processing in a sequence of stages:

- Stage 0—Server Started
- Stage 1—Trust Certificates
- Stage 2—CRL Received/Validated
- Stage 3—CRT/OCSP Request Received
- Stage 4—OCSP/IP Request Authentication
- Stage 5—Certificate Status Lookup
- Stage 6—OCSP Response Signing

An extension can extend the Enterprise VA processing at any of these stages to include processing that is specific to the extension.

NOTE: The extension, has complete flexibility in selecting the stages that it wants to extend and the level of processing it wants to perform at a particular stage.

An extension can add its own functionality to the Enterprise VA by providing an event handler. Each Enterprise VA stage maps to an event contained in bit mask. An extension indicates to the Enterprise VA that it is interested in being notified when the Enterprise VA has reached a particular stage and that the extension will provide some processing for that stage. An extension can do this by setting the value of the bit mask to include the value of a specific event. When the Enterprise VA reaches that stage, it calls the event handler, which then performs its processing and returns to the Enterprise VA. The Enterprise VA resumes its request processing at the point it called the extension. If multiple extensions want to be called at the same stage, the Enterprise VA chains the calls to the extensions together, and processes the requests in sequence.

NOTE: If an extension within a chain returns the EVA_EXT_STATUS_FAILURE error code, processing for the entire chain is terminated. It is recommended that extensions return the EVA_EXT_STATUS_CONTINUE_PROCESSING error code, instead.

The Enterprise VA supports multiple threads, and processes each request in the context of its thread, which makes it thread safe.

Table 4 lists the events that map to the various Enterprise VA processing stages and their bit value within the bit mask.

Table 4. Stage to Event Mapping

Stage	Value	Event
0	0x2000	EVA_EXT_NOTIFY_SERVER_STARTED
1	0x0010	EVA_EXT_NOTIFY_TRUST_CERTS
2	0x0001 0x0002	EVA_EXT_NOTIFY_ALL_CRT_REQUESTS EVA_EXT_NOTIFY_ALL_OCSP_REQUESTS

Table 4. Stage to Event Mapping (Continued)

Stage	Value	Event
3	0x4000 0x8000	EVA_EXT_NOTIFY_ALL_CRL_VALIDATED EVA_EXT_NOTIFY_ALL_CRL_RECEIVED
4	0x0008 0x1000	EVA_EXT_NOTIFY_OCSP_REQUEST_AUTH VA_EXT_NOTIFY_IP_AUTH
5	0x0020	EVA_EXT_NOTIFY_LOOKUP_CERT_STATUS
6	0x0080	EVA_EXT_NOTIFY_SIGN

For a description of each of these events, see “Event Notification Types” on page 115.

Basic Extension Tasks

When you write your extension to extend the Enterprise VA request processing, the extension must perform some basic tasks to interface with the Enterprise VA. These include the following:

- Register with the Enterprise VA
- Pass data to and from the Enterprise VA
- Manage memory

The tasks listed in this procedure are also indicated in the sample extension.

To interface with the Enterprise VA

Step 1 Register extension with the Enterprise VA

When your extension registers with the Enterprise VA, the extension establishes its version, description, and most importantly the events its is interested in. Use the `GetEVAExtensionVersion` function to to register your extension with the Enterprise VA. See //STEP 1 in the sample extension.

Once the your extension is registered, the Enterprise VA notifies the extension when it reaches each stage that corresponds to an event specified in the `GetEVAExtensionVersion` function.

For information about this function, see “GetEVAExtensionVersion” on page 113.

Step 2 Pass data between the extension and the Enterprise VA.

Your extension and the Enterprise VA can pass event-specific data using the EVAExtensionProc function at various stages of the Enterprise VA request processing. See //STEP 2 in the sample extension.

For information about this function, see “EVAExtensionProc” on page 110.

Step 3 Release the memory allocations.

Your extension must call this function to release memory allocated to the extension by the Enterprise VA. The Enterprise VA calls this function before it unloads the extension. The extension can perform any cleanup operations it needs to before the Enterprise VA unloads the extension. See //STEP 3 in the sample extension.

For information about this function, see “FreeEVAExtension” on page 112.

Loading the Extension

Once you have written your extension, it must be loaded before the Enterprise VA can integrate it into its request processing. To load it, you must place the DLL or shared object and its `.ecf` file in the `enterpriseva/entserv` directory. This allows you to add and delete your extension through the Enterprise VA Administration Server. I

The `valicert.ini` file should have an entry for each extension indicating the `.dll` or `.so` that needs to be loaded. The entry would be similar to the following:

```
EVAExtensions= “thirdparty.dll”
```

You can provide a `.ini` file which could be appended to the valicert.ini file as a section. The section would be added using the extension name.

Sample Extension

```
#ifdef WIN32

    #include <windows.h>

#endif

#include <stdio.h>
#include <ctype.h>
#include <time.h>
#include <sys/types.h>
#include <sys/stat.h>

extern “C” {
#include <err.h>
#include <bn.h>
#include <rsa.h>
#include <txt_db.h>
#include “evp.h”
#include <crypto.h>
#include <x509.h>
#include <objects.h>
#include <pem.h>
#include <buffer.h>
#include <ocsp.h>
}

// locking specifically for SSLeay
void thread_setup();
void extension_locking_callback(int mode, int type, char* file, int line);
void thread_cleanup();

// Simple Thumbrules for memory allocations in Extensions

// if using ssleay functions use the crypto_set_mem functions to the ones
//passed to the extension from the server. This way the ssleay
//allocation/deallocation will work across the server and the extension in a
//seamless manner. i.e. memory allocated by the extension could be freed by
//the server

// If you need to allocate memory locally in the extension which could be used
//by the c-runtime use malloc/free etc. using the extension provided
//malloc/free does not work with c-runtime like fwrite(...) etc.
```

```
// if you need to return data back to the server use the ext provided
//mechanism.


#ifdef WIN32

int APIENTRY
DllMain( void* hModule, unsigned long ul_reason_for_call, void* lpReserved )
{
   switch( ul_reason_for_call ) {
     case DLL_PROCESS_ATTACH:
         break;
     case DLL_PROCESS_DETACH:
        break;
     default :
        break ;
   }
   return TRUE;
}
#endif /* WIN32 */


// Only for SSLeay, because malloc is defined with a char* instead of void *
typedef char *(*ssleay_malloc)();
typedef char *(*ssleay_realloc)();
typedef void  (*ssleay_free)();

eva_log g_evaLogFn;
eva_free g_evaFreeFn;

struct proxyHandle
{

 char *data;
};

extern "C"
{
void SSLeay_add_all_algorithms(void);
}


pVer->dwFlags = EVA_EXT_NOTIFY_ALL_CRT_REQUESTS |
EVA_EXT_NOTIFY_ALL_OCSP_REQUESTS | EVA_EXT_NOTIFY_PROCESS_ERRORS |
EVA_EXT_NOTIFY_TRUST_CERTS | EVA_EXT_NOTIFY_OCSP_REQUEST_AUTH |
EVA_EXT_NOTIFY_LOOKUP_CERT_STATUS | EVA_EXT_NOTIFY_OCSP_OID |
EVA_EXT_NOTIFY_LOGGING |EVA_EXT_NOTIFY_SEND_RESPONSE |
EVA_EXT_NOTIFY_PROXY_REQUEST  | EVA_EXT_NOTIFY_SIGN;

//STEP 1
int GetEVAExtensionVersion(PEVA_EXTENSION_VERSION pVer)
{
    int rv =0;

    rv = pVer->evaLicenseCheck("sampleExtension");

    if(rv == 0)
    {
        pVer->evaLog(EVA_EXT_LOG_WARNING, "No License found for the
extension");
        return FALSE;
    }

    thread_setup();// calling thread lock setup routines

    CRYPTO_set_mem_functions((ssleay_malloc)pVer-
>evaAlloc,(ssleay_realloc)pVer->evaRealloc, (ssleay_free)pVer->evaFree);

    SSLeay_add_all_algorithms();

    g_evaLogFn = pVer->evaLog;
    g_evaFreeFn = pVer->evaFree;

    proxyHandle *pHandle=NULL;
    pHandle = (struct proxyHandle *)pVer->evaAlloc(sizeof(struct
proxyHandle));

    memset(pHandle, '\0', sizeof(struct proxyHandle));

    pVer->hDLLContext = (void *)pHandle;

    pVer->dwFlags =   EVA_EXT_NOTIFY_IP_AUTH  |
EVA_EXT_NOTIFY_OCSP_REQUEST_AUTH | EVA_EXT_NOTIFY_ALL_OCSP_REQUESTS |
EVA_EXT_NOTIFY_ALL_CRT_REQUESTS;

    strcpy(pVer->lpszExtensionDesc, "sampleExtension");
    pVer->dwExtensionVersion= 1;

    pVer->evaLog(EVA_EXT_LOG_INFO, "sampleExtensions :: Extension
successfully initialized \n");

    return TRUE;
```

```
}

//STEP 2
unsigned long  EVAExtensionProc(void* hConn,
                        void *pfc, /* EVA server allocated data*/
                        unsigned long notificationType,
                        void **pvNotification,
                        eva_alloc evaAlloc,
                        eva_realloc evaRealloc,
                        eva_free evaFree,
                        eva_read_config_int evaReadConfigInt,
                        eva_read_config_string evaReadConfigString,
                        eva_log                evaLog
                       )
{

    proxyHandle *pHandle;

    pHandle = (struct proxyHandle *)hConn;


    if(pHandle == NULL)
        return EVA_EXT_STATUS_FAILURE;

    unsigned long retVal = 0;
    switch(notificationType)
    {

        case  EVA_EXT_NOTIFY_OCSP_REQUEST_AUTH  :
        {
            X509_OCSP_REQUEST *pRequest;

            pRequest = (X509_OCSP_REQUEST *)pfc;

          if (VerifySignatureOnRequest(pRequest, pHandle->pTrustedClientCAs,
pHandle->pTrustedVAs) == TRUE)
            {
                retVal = EVA_EXT_STATUS_SUCCESS;

            }
            else
            {
                evaLog(EVA_EXT_LOG_INFO, "Failure in Request Signature
verification\n");
                retVal = EVA_EXT_STATUS_FAILURE;
            }
        }
        break;

        case EVA_EXT_NOTIFY_ALL_OCSP_REQUESTS :
            {

                X509_OCSP_REQUEST *pRequest;

                pRequest = (X509_OCSP_REQUEST *)pfc;

                unsigned char *reqDer = NULL, *cp;
                int reqLen = i2d_X509_OCSP_REQUEST(pRequest, NULL);

                reqDer = (unsigned char *)malloc(reqLen+1);

                cp = reqDer;

                reqLen = i2d_X509_OCSP_REQUEST(pRequest, &cp);

                //  just log it to a database, non repudiation
                // can do better database  management like storing it in a
                // cache and dumping it maybe 100 records at a time.

                // implement a simple mutex in the future

                FILE * fp = fopen("ocsp", "a+b");

                fwrite( reqDer, reqLen, 1, fp );

                fclose(fp);

                // nothing about the response returned.
                // we will see in the future is something has to be returned.

                 free(reqDer);
                 retVal = EVA_EXT_STATUS_SUCCESS;
            }
            break;

        case EVA_EXT_NOTIFY_ALL_CRT_REQUESTS :
            {
                X509_CONFIRM_REQ *pRequest;

                pRequest = (X509_CONFIRM_REQ *)pfc;
                unsigned char *reqDer = NULL, *cp;
                int reqLen = i2d_X509_CONFIRM_REQ(pRequest, NULL);

                reqDer = (unsigned char *)malloc(reqLen+1);

                cp = reqDer;

                reqLen = i2d_X509_CONFIRM_REQ(pRequest, &cp);

                //  just log it to a database, non repudiation
                // can do better database  management like storing it in a
                // cache and dumping it maybe 100 records at a time.

                // implement a simple mutex in the future

                FILE * fp = fopen("crt", "a+b");

                fwrite( reqDer, reqLen, 1, fp );

                fclose(fp);

                // nothing about the response returned.
                // we will see in the future is something has to be returned.

                 free(reqDer);
                 retVal = EVA_EXT_STATUS_SUCCESS;
            }
            case  EVA_EXT_NOTIFY_LOOKUP_CERT_STATUS :
            {
                X509_CONFIRM_REQ *pRequest;
                X509_CONFIRM *pConfirm;

                pRequest = (X509_CONFIRM_REQ *)pfc;

                pConfirm = X509_CONFIRM_new();

                if(!pConfirm)
                    return(FALSE);

                int rv = ASN1_ENUMERATED_set(pConfirm->resultStatus, 1);
/* Set all certificates as revoked */
                if(!rv)
                {
                    X509_CONFIRM_free(pConfirm);
                    return(FALSE);
                }
                *(X509_CONFIRM **)pvNotification = pConfirm;

            }
            retVal = EVA_EXT_STATUS_SUCCESS;
            break;
        }

    return retVal;
}


//STEP 3
int FreeEVAExtension(void *pfc)
{

    proxyHandle *pHandle;
    pHandle = (struct proxyHandle *)pfc;

    if(pHandle != NULL)
    {
        g_evaFreeFn(pHandle);
    }
    thread_cleanup();
    return TRUE;
}


/* Thread Safety example using CAmMutex (a sample mutex implementation */
/* change CAmMutex to whatever mutex implementation you feel is appropriate
*/


static CAmMutex *pThreadSafetyMutex[CRYPTO_NUM_LOCKS];

void thread_setup()
{

    for (int i=0; i<CRYPTO_NUM_LOCKS; i++)
    {
   pThreadSafetyMutex[i] = new CAmMutex();
    }

    CRYPTO_set_locking_callback((void (*)(int,int,char
*,int))extension_locking_callback);
   /* id callback defined */
```

```
}

void thread_cleanup()
{
    for (int i=0; i<CRYPTO_NUM_LOCKS; i++)
    {

   if(pThreadSafetyMutex[i])
            delete pThreadSafetyMutex[i];
    }
}

void extension_locking_callback(int mode, int type, char* file, int line)
{
    AMNOTUSED(file);
    AMNOTUSED(line);

    if (mode & CRYPTO_LOCK)
    {
   pThreadSafetyMutex[type]->Lock();
    }
    else
    {
   pThreadSafetyMutex[type]->Unlock();
    }
}
```

CHAPTER
6

VA API Reference

This section provides reference information about data structures, functions, error codes, and notification types available to developers who are implementing a VA extension.

For task-oriented information on how to use these functions in your application, refer to Chapter 5, "Writing a VA Extension."

Data Structures

The VA API provides several data structures that are used by the VA API functions. The data structure can have one of the following type definitions:

- integer (signed and unsigned)
- structure
- char (signed and unsigned)

_EVA_EXTENSION_VERSION

```
typedef struct _EVA_EXTENSION_VERSION{
   unsigned long dwServerEVAVersion; //input
   unsigned long dwSExtensionVersion; //output
   char lpszExtensionDesc
     [EVA_MAX_EXTENSION_DESC_LEN+1]; //output
   char sxReserved [64]; //input
   unsigned long dwFlags; //output
   void *hDLLContext; //output
   eva_alloc evaAlloc; //input
   eva_realloc evaRealloc; //input
   eva_free evaFree; //input
   eva_read_config_int evaReadConfigInt; //input
   eva_read_config_string evaReadConfigString;
   //input
   eva_log evaLog; //input
   eva_licensecheck evaLicenseCheck; //input
} EVA_EXTENSION_VERSION, *PEVA_EXTENSION_VERSION;
```

Description

This structure is used to notify the Enterprise VA about the extension. It contains information such as the server version, extension version, description of the extension, and which events the extension wants to be notified about from the Enterprise VA.

It is used in the GetEVAExtensionVersion function.

Parameters

dwServerEVAVersion	Version of the Enterprise VA server.
dwSExtensionVersion	Version of the extension
lpszExtensionDesc	Location in which to store a description of the EVA extension. It can be up to 64 characters in length.
sxReserved	Reserved for future use.

dwFlags

Bit mask to indicate which events the extension is interested in. These events map to an Enterprise VA processing stage. The possible events areas follows:

- EVA_EXT_NOTIFY_SERVER_STARTED
- EVA_EXT_NOTIFY_TRUST_CERTS
- EVA_EXT_NOTIFY_ALL_CRT_REQUESTS
- EVA_EXT_NOTIFY_ALL_OCSP_REQUESTS
- EVA_EXT_NOTIFY_ALL_CRL_VALIDATED
- EVA_EXT_NOTIFY_ALL_CRL_RECEIVED
- EVA_EXT_NOTIFY_OCSP_REQUEST_AUTH
- EVA_EXT_NOTIFY_IP_AUTH
- EVA_EXT_NOTIFY_LOOKUP_CERT_STATUS
- EVA_EXT_NOTIFY_SIGN

For information about these events, see “Event Notification Types” on page 115.

hDLLContext

Context returned by the extension during initialization. The Enterprise VA maintains the context and passes it back to the extension at every stage at which the extension has requested to be called.

evaAlloc

Function pointer passed by the Enterprise VA to the extension. The extension uses it to allocate memory in the Enterprise VA process space. This does not affect memory in the extension process space.

evaRealloc

Function pointer passed by the Enterprise VA to the extension. The extension uses it to reallocate memory in the Enterprise VA process space. This does not affect memory in the extension process space.

evaFree

Function pointer passed by the Enterprise VA to the extension. The extension uses it to free memory in the Enterprise VA process space. This does not affect memory in the extension process space.

evaReadConfigInt

Function pointer passed by the Enterprise VA to the extension. The extension uses it to read integers in the `valicert.ini` file.

evaReadConfigString

Function pointer passed by the Enterprise VA to the extension. The extension uses it to read strings in the `valicert.ini` file.

evaLog

Function pointer passed by the Enterprise VA to the extension. The extension uses it to place messages into the EVA logs. For information about the EVA logs, see “Viewing Logs” on page 91.

evaLicenseCheck	Function pointer passed by the Enterprise VA to the extension. The extension uses it to pass its license information to the Enterprise VA.

Notes

None

See Also

None

Functions

The functions are described in alphabetical order. The following functions are available:

- EVAExtensionProc
- FreeEVAExtension
- GetEVAExtensionVersion

EVAExtensionProc

```
#include <evaapi.h>

unsigned long EVAExtensionProc(
   void* hDLLContext,                //input
   void *pfc,                        //input
   unsigned long notificationType,    //input
   void **pvNotification,          //input/output
   eva_alloc evaAlloc,               //input
   eva_realloc evaRealloc,           //input
   eva_free evaFree,                 //input
   eva_read_config_int evaReadConfigInt,   //input
   eva_read_config_string evaReadConfigString,
   //input
   eva_log evaLog                  //input
);
```

Description

This function allows the Enterprise VA and extension to pass event specific data between them at various stages of the Enterprise VA request processing.

Parameters

hDLLContext
The data area pointed to by this parameter contains DLL context specific information which is any information created by the extension during its initialization.

pfc
Points to Enterprise VA allocated data. This structure contains event specific parameters.

notificationType
Notification type that is currently being processed.

pvNotification
Points to notification-specific structure which the extension returns to the Enterprise VA.

evaAlloc
Memory allocation function provide by the Enterprise VA.

evaRealloc
Memory allocation function provide by the Enterprise VA.

evaFree
Memory allocation function provide by the Enterprise VA.

evaReadConfigInt
Configuration function provide by the Enterprise VA.

evaReadConfigString	Configuration function provide by the Enterprise VA.
evaLog	Log function provide by the Enterprise VA.

Return Value

See “Extension Error Codes” on page 114.

Notes

None

See Also

“FreeEVAExtension” on page 112

“GetEVAExtensionVersion” on page 113

FreeEVAExtension

```
    #include <evaapi.h>

    int FreeEVAExtension(void *pfc);    //input
```

Description

This function releases memory allocated to the extension by the Enterprise VA. The extension calls this function before the Enterprise VA unloads the extension. The extension can perform any cleanup operations it needs to before the Enterprise VA unloads the extension.

Parameters

pfc	Points to the structure passed in the EVAExtensionProc function by the Enterprise VA. This structure contains event specific parameters.

Return Value

See “Extension Error Codes” on page 114.

Notes

None

See Also

“EVAExtensionProc” on page 110

“GetEVAExtensionVersion” on page 113

GetEVAExtensionVersion

```
#include <evaapi.h>

int GetEVAExtensionVersion(
   PEVA_EXTENSION_VERSION *pVer //input/output
);
```

Description

This function registers the extension with the Enterprise VA. It is the first entry point into your extension that the Enterprise VA calls. The extension uses this function to specify which events it is interested in and therefore at which stages the Enterprise VA should call the extension.

Parameters

pfc	Pointer to the `PEVA_EXTENSION_VERSION` contains structure which contains information such as the server version, extension version, description of the extension, and which events the extension wants to be notified about from the Enterprise VA.

Return Value

The return code indicates whether the extension was properly loaded.

If the extension returns TRUE, the extension will be loaded and receives notifications from the Enterprise VA. If the extension returns FALSE, the extension will be unloaded and will not receive notifications from the Enterprise VA.

Notes

Some events are potentially resource intensive in that they require significant CPU resources and greater I/O throughput. These notifications can significantly affect the speed and scalability of the Enterprise VA. Therefore, extensions should register for only those events that are required.

See Also

“EVAExtensionProc” on page 110

“FreeEVAExtension” on page 112

Extension Error Codes

Table 5 lists and briefly describes the error codes that an extension can return to the Enterprise VA. These error codes determine whether the Enterprise VA continues to include the extension in its request processing.

Table 5. Extension Error Codes

Error Codes	Description
EVA_EXT_STATUS_SUCCESS	Stop processing the request at the stage and return immediately to the send stage
EVA_EXT_STATUS_FAILURE	Stop processing the request at the stage, and return immediately to the send stage, indicating errors. If multiple extensions have requested notification at the same stage, this status will terminate the chain of call backs for that stage.
EVA_EXT_STATUS_STAGE_OVER	Do not call any more extensions for this stage, go to next stage
EVA_EXT_STATUS_CONTINUE_PROCESSING	Continue processing the request to any more extensions of the is stage itself or the next stage if this stage is over
EVA_EXT_STATUS_STAGE_SIGN	Jump to the signing stage.

Event Notification Types

This section describes each of the event notification types. The extension uses these event notification types to specify which events it wants to be notified about by the Enterprise VA. These event notification types correspond to various Enterprise VA request processing stages.

The extension specifies these events in the GetEVAExtensionVersion function.

NOTE: The `evaapi.h` file currently contains 17 event notification types. However, your extension can only use the ones that are listed and described in this section. Those not listed here, are reserved for ValiCert use only.

EVA_EXT_NOTIFY_ALL_CRL_RECEIVED

This event gets invoked when the Enterprise VA receives a CRL or a CRL/DP from the ValiCert VA Publisher. The Enterprise VA passes to the extension the DER-encoded CRL data. The Enterprise VA passes the data in the CRL_DATA_EXT structure, which is defined in the `evaapi.h` file.

This event corresponds to stage 3 of the Enterprise VA request processing.

EVA_EXT_NOTIFY_ALL_CRL_VALIDATED

This event gets invoked when the Enterprise VA receives a CRL or a CRL/DP from the ValiCert VA Publisher. The Enterprise VA passes to the extension the DER-encoded CRL data and the certificate that signed the CRL. The Enterprise VA passes the data in the CRL_DATA_EXT structure, which is defined in the `evaapi.h` file.

This event corresponds to stage 3 of the Enterprise VA request processing.

EVA_EXT_NOTIFY_ALL_CRT_REQUESTS

This event gets invoked when the Enterprise VA receives any CRT request. The Enterprise VA passes to the extension the CRT date. The Enterprise VA passes the data in the X509_CONFIRM_REQUEST structure, which is defined in the `ocspi.h` file.

This event corresponds to stage 2 of the Enterprise VA request processing.

EVA_EXT_NOTIFY_ALL_OCSP_REQUESTS

This event gets invoked when the Enterprise VA receives any OCSP request. The Enterprise VA passes to the extension the OCSP data. The Enterprise VA passes the data in the X509_OCSP_REQUEST structure, which is defined in the `ocsp.h` file.

This event corresponds to stage 2 of the Enterprise VA request processing.

EVA_EXT_NOTIFY_IP_AUTH

This event gets invoked when the Enterprise VA authenticates requests. The Enterprise VA can perform access control based on the IP address of the requester to shut down attacks from IP addresses. The IP authentication occurs immediately after the connection is established to allow the extension to block attacks before it has accepted any invalid CRL requests.

The Enterprise VA passes the data in the `in_addr` structure, which is defined in the `socket.h` file.

This event corresponds to stage 4 of the Enterprise VA request processing.

EVA_EXT_NOTIFY_LOOKUP_CERT_STATUS

This event allows the extension to provide validation information based on custom schemes specific to the extension. For example, the extension could use this event to access a CA database, or override CRLs for specific CAs that the VA chooses not to trust. This stage can also act like a proxy and service the request by contacting another VA.

The Enterprise VA passes to the extension an OCSP request. The Enterprise VA passes the data in `the X509_SINGLE_OCSP_REQUEST_st` structure, which is defined in the `evaapi.h` file.

This event corresponds to stage 5 of the Enterprise VA request processing.

EVA_EXT_NOTIFY_OCSP_REQUEST_AUTH

This event gets invoked when the Enterprise VA authenticates requests. The Enterprise VA can authenticate signed OCSP requests. The OCSP authentication occurs immediately after the connection is established to allow the extension to block attacks before it has accepted any invalid OCSP/CRT requests.

The Enterprise VA passes the data in the `X509_OCSP_REQUEST` structure, which is defined in the `ocsp.h` file.

This event corresponds to stage 4 of the Enterprise VA request processing.

EVA_EXT_NOTIFY_SERVER_STARTED

This event gets invoked after all the extensions are successfully loaded, but before the Enterprise VA begins accepting validation requests or CRLs.

The Enterprise VA does not pass a structure to the extension.

This event corresponds to stage 0 of the Enterprise VA request processing.

EVA_EXT_NOTIFY_SIGN

This event indicates that the extension is interested in signing the response. The Enterprise VA passes the request to the extension. The Enterprise VA passes the request in a `X509_OCSP_REQUEST` structure, which is defined in the `ocsp.h` file. When the extension completes its processing successfully, it returns the X509_BASIC_OCSP_RESPONSE to the Enterprise VA. A successful return value indicates that the Enterprise VA should not sign the response.

This event corresponds to stage 6 of the Enterprise VA request processing.

EVA_EXT_NOTIFY_TRUST_CERTS

This event gets invoked when the Enterprise VA starts initially. The Enterprise VA calls the extension to get any additional certificates that the extension wants the Enterprise VA to trust. The extension is not restricted where it can get these additional certificates. The Enterprise VA and extension use a stack* to pass the certificates.

This event corresponds to stage 1 of the Enterprise VA request processing.

CHAPTER 7

Using the Directory Update Extension

This section describes the ValiCert Directory Update extension which is provided as part of the Enterprise VA package. It can be installed during installation of the Enterprise VA. This extension provides an open storage format for CRL and CRLdp data, so that the data may be accessed by other applications. This extension uses the VA API in the same way described in Chapter 5, "Writing a VA Extension." It must do the following:

- Register with the Enterprise VA
- Pass data between the extension and the Enterprise VA
- Release memory allocations.

Features

This extension enhances the functionality of Enterprise VA in the following ways:

- Adds LDAP (light-weight direct access protocol support) to Enterprise VA
- Adds CRL and CRLdp support to Enterprise VA via LDAP protocol

The Directory Update extension is implemented as a standalone dynamic library `ldapcrl.dll` or a shared object named `ldapcrl.so`. The extension interfaces to the Enterprise VA through the VA API.

In addition, you can configure the extension parameters and output logging using the standard Enterprise VA Administration Server interface.

NOTE: All CRLLDAP configuration properties are prefixed with `ldap`, for example, `ldapServerHost` and they are contained in the `[LdapDirectory]` section of the `valicert.ini` file.

Directory Update extension also features the following:

- CRLdp and CRL storage in the Directory Server

  CRLdp and CRLs are stored in the directory server and are available through a CRL and CRLdp lookup.
- Built upon Netscape's SDK/libraries/server
- Non-secure data transfer, for example, non-SSL
- Uses LDAP version 2 feature set
- Uses directory permissions for security
- CRL stored in DER format by issuer's DN
- User/password based authentication
- Single threaded operation

How the Directory Update Extension Works

The extension enables all CRLs and CRLdps coming to the Enterprise VA to be posted to the directory server. This means, as the ValiCert VA Publisher posts CRLs and CRLdps to the Enterprise VA, the Directory Update extension can post CRLs and CRLdps to the directory server.

For example, when the VA Publisher sends a Full CRL or CRLdp to the Enterprise VA, the Enterprise VA validates the CRL. If the Directory Update extension is configured on the Enterprise VA, the VA sends the CRL to the extension, which then writes the data to the directory.

Specifically, the Enterprise VA Directory Update extension does the following:

Step 1 Examines the CRL/CRLdp posted by the VA Publisher and identifies whether it is a CRL or CRLdp.

Step 2 If it is a full CRL, the extension looks for the DN of the CA that issued the CRL. If the DN is not already present, the extension creates a DN under which the CRL is to be stored for the CA that issued the CRL. If it is a CRLdp, the CRLdp it will be stored under the DN specified in the CRLdp. If the DN is not present in the issuing distribution point extension, the CRLdps are stored in the same DN as the issuer’s DN.

Step 3 Posts CRLs/CRLdp to the directory server.

Step 4 Logs the post and response from directory server in a log file. It logs:

a CRL/CRLdps posted to the directory.

b Responses from the directory.

Figure 4 shows this transaction.

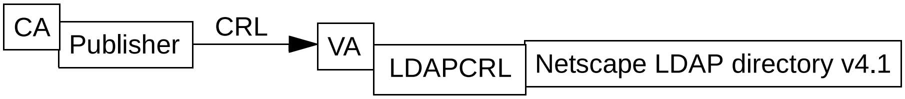


Figure 4. Transaction using Directory Update Extension

NOTE: The Directory Update extension currently uses the Netscape Directory Server as the directory storage mechanism to store and serve up the CRLs and CRLdp for the CAs handled by the Enterprise VA.

Loading the Directory Update Extension

The Enterprise VA server installer installs the LDAP server and copies any required dynamic libraries to the appropriate locations. In addition, when the extension is added through the Enterprise VA, the default CRLLDAP property values are added to the Enterprise VA initialization file.

The installer will append the following to the `valicert.ini` file for the extension, indicating that the `.dll` or `.so` needs to be loaded. The entry would be similar to the following:

```
[ves]
...
ExtensionDLL = ldapcrl.dll  // enables LDAPCRL
ldapServerHost = <servername[:port_number]> default
localhost:389
ldapUser = <user name used to connect to ldap server>
ldapPassword = <password used to connect to ldap server>
...
```

The Directory Update extension is enabled by providing the name of the extension library (ldapcrl.dll or ldapcrl.so) in the server initialization file. After the library is successfully loaded, the Enterprise VA will notify LDAPCRL under the following conditions:

- Server Initialization
- CRL Updates
- Server Shutdown

Server Initialization

LDAPCRL initialization is performed when the server calls the library's GetEVAExtensionVersion function. This routine will attempt to establish a connection to the LDAP server and create DNs of CAs trusted by the Enterprise VA. For more information about this function, see “EVAExtensionProc” on page 110.

If data can be written to the server, the extension will specify that it should be notified following the validation of all new CRL/CRLdp using EVA_EXT_NOTIFY_ALL_CRL_VALIDATED. For more information about this notification type, see “EVA_EXT_NOTIFY_ALL_CRL_VALIDATED” on page 115.

If it is not possible to write data to the server, the initialization will return FALSE and the server will halt after writing a message to the log file. The LDAP server connection is closed at the end of the initialization routine. In order to facilitate debugging, the status of all LDAP operations are logged.

The LDAP connection state data, for example, user, password and server name are obtained from the [LdapDirectory] section of the valicert.ini using the following properties:

- ldapServerHost
- ldapUser
- ldapPassword

While the ldapServerHost option allows the specification of a remote LDAP server, standard operation is to run it on the same machine as the Enterprise VA server.

The default LDAP port (for example, 389) is used, unless an alternate port is specified by appending the server name with ":<port_number>".

User authentication is enforced by password checking and must have write privileges into the LDAP server. CRL data protection is limited to any access restrictions enforced by the LDAP server.

CRL Updates

Assuming a successful initialization, the server will call the main `LDAPCRL` handler function (`EVAExtensionProc`) following the validation of a new CRL. Passed as part of the calling signature are references to the `DER` encoded CRL data and its corresponding X.509 representation. The CRL data is written as `BER` (binary) data into a top level directory specified by the issuer's distinguished name. CRLdps are written in the DN specified in the issuing distribution point extension specified in the CRLdp. If the DN is not present in the issuing distribution point extension, the CRLdps are stored in the same DN as the issuer’s DN.

A status line is written to the log file, both before and after calling the LDAP update routine. No history mechanism is kept for the CRL data, an update to a list destroys any previously recorded data.

Server Shutdown

The server calls `FreeEVAExtension` when shutting down. This routine frees system resources. The persistent connection option also closes the connection to the LDAP server.

Configuring the Directory Update Extension

The Directory Update extension has a forms-based interface for configuring the extension. The extension has a configuration file to control the CRL and CRLdp in the directory. You can configure the following features of the directory server:

- One-time priming of the Enterprise VA (via the Enterprise VA)
- Login/Password for Enterprise VA to configure LDAP (via Setup)

APPENDIX

A

Using Delegated Certificates

This section describes the procedures to issue and obtain a delegated certificate for the ValiCert Enterprise VA. A delegated Enterprise VA certificate is one that is signed by a CA (thereby delegated the trust to the Enterprise VA). A delegated server certificate is signed by a local CA or by a public CA. This chapter describes the procedures for issuing and retrieving delegated certificates from local CAs.

NOTE: To submit your certificate request to a public CA (like VeriSign or CyberTrust) contact that CA for their specific instructions.

Make sure the certificate includes the fields specified in Table 6, “Extension Fields for Delegated Certificates,” on page 126.

There are two steps, one is issuing a delegated certificate and the other is retrieving delegated certificates.

To illustrate the procedures the following specific examples are included:

Baltimore UniCERT CA —issuing

Entrust/PKI—issuing

Netscape CMS 4.x—retrieving

Microsoft Certificate Server 1.1—retrieving

Introduction

Delegated certification provides a trust model that roots the VA and client applications to the same trust point.

In the direct trust model, the VA and the client application have no common trust point. A CA's root certificate must be installed in the ValiCert Enterprise VA certificate store so it recognizes CRLs sent by the CA.

The ValiCert Enterprise VA uses a self-signed certificate which is generated and signed by the Enterprise VA to sign responses to the client. The client application must include the VA's self-signed certificate and the root certificate of the certificate authority's (CA's) that publishes revocation information in its trust path.

In the delegated certification model, the VA uses the certificate that is signed by the trusted CA to sign validation responses. In this case, the client application only needs the CA root certificate in order to trust the responses from the ValiCert Enterprise VA.

Certificate Requirements

Delegated certificates require CAs to issue extension fields to VA server certificates. Table 6 lists the required extension fields.

Table 6. Extension Fields for Delegated Certificates

Extension Name	OID	Usage	Remark
Extended Key Extension	2.5.29.37	OCSP Responder	Optional Certificate Extensions
OCSP Signing	1.3.6.1.5.5.7.3.9	OCSP Responder	Required Certificate Extensions
OCSP Nocheck	1.3.6.1.5.5.7.48.1.5	OCSP Root Responder	Optional Certificate Extensions
Authority Information Access (AIA)	1.3.6.1.5.5.7.1.1	Root and immediate CA	Optional Certificate Extensions

Issuing Delegated Certificates

You can configure your local CA to issue delegated certificates. To do this you must configure your CA so that it adds the fields described in Table 6 to the certificates it issues.

Instructions on how to configure Baltimore UniCERT and Entrust/PKI are provided as examples of how to configure a CA to issue delegated certificates.

Baltimore UniCERT

This section describes how to use delegated certificates from the Baltimore UniCERT CA. It contains information about the following:

- Prerequisites
- Issuing a Delegated Certificate

Prerequisites

- Installed Oracle database server (v8.05).
- Installed Baltimore UniCERT CA/RA/CAO/RAO (v3.0).

NOTE: Baltimore UniCERT 3.0x or later versions contain the fix for generating an AIA extension for the root CA certificate.

Issuing a Delegated Certificate

To obtain a delegated certificate

Step 1 Create a PKI policy with PKI Editor from the CA Operator

(Please refer to page 6 in the “PKI Design and Initialization” section of the *UniCERT User Guide, Version 3.0 Certification Authority Operation*). See Figure 5 and Figure 6.

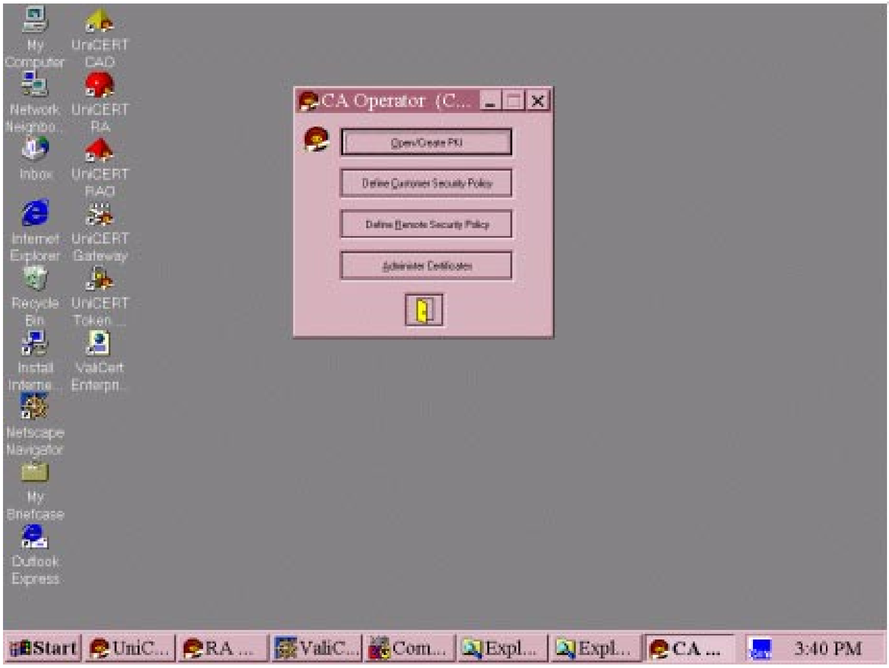


Figure 5. Launch the PKI Editor from CA Operator

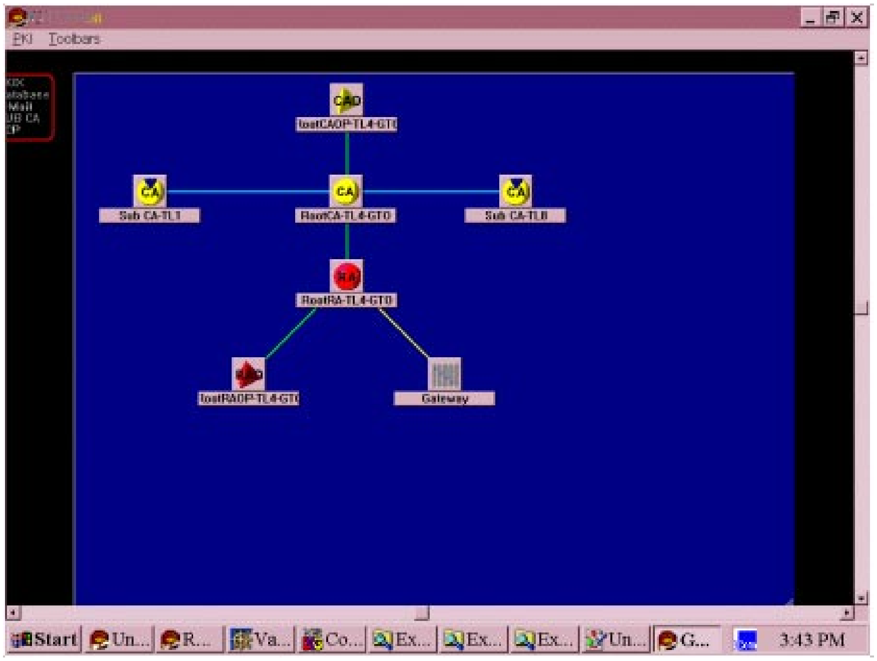


Figure 6. Baltimore UniCERT CA PKI Editor Workspace

Step 2 Create a Policy with the Policy Editor (*see Diagram 3, below*).

(Please refer to page 38 in the “Defining Policies for Certification” section of the *UniCERT User Guide, Version 3.0 Certification Authority Operation*).

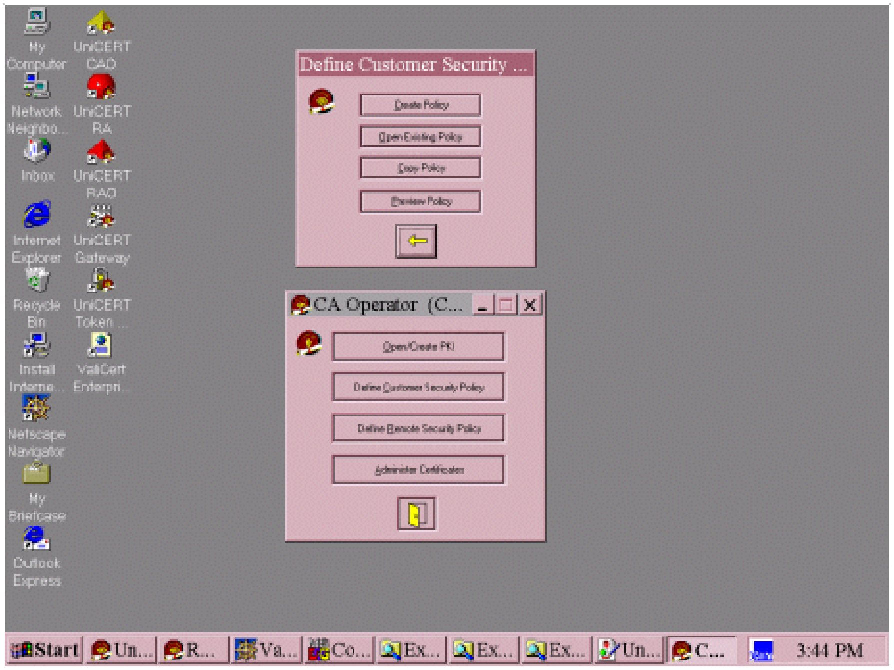


Figure 7. Launch the Policy Editor from CA Operator

Step 3 Add the certificate extension with the Attributes Toolbar. Instructions for each type of extension follow below:

AIA

a Select **AIA** icon.

b Drag and drop the icon into the workspace.

c Edit the property by entering the URL. For example:

```
http://www.valicert.com:80
```

Extended Key Usage – OCSP Server (OCSP Signing)

a Select the **Extended Key Usage** icon.

b Drag and drop the icon into the workspace.

c Highlight the OCSP Server.

Generic Extensions – OCSP No Check

a Select **Generic Extension**.

b Drag and drop the extension into the workspace.

c Edit the property by entering the OID 1.3.6.1.5.5.7.48.1.5

NOTE: You need to push the policy by using the PKI Editor.

(Please refer to page 60 of the “Pushing Policies to RA Operators” section in the *UniCERT User Guide, Version 3.0 Certification Authority Operation*).

Entrust/PKI

To issue delegated certificates

Step 1 Export the certificate specification file by selecting **export certificate specifications** under file menu of Entrust/admin and save the file.

Step 2 Open the file with text editor.

Step 3 Add certificate type by adding the following line under the section of Certificate Types section:

```
valicert_ocsp=web, valicert ocsp, valicert ocsp
responder certificates
```

Step 4 Add the OCSP extensions.

Step 5 Adding the following lines after last line of the Certificate Type section:

```
            [valicert_ocsp Verification Extensions]

            ;
--------------------------------------------------------

            ; <ASN1> extKeyUsage::=SEQUENCE {id-kp-9}

            ;
 -------------------------------------------------------


extKeyUsage=2.5.29.37,n,DER,300A06082B06010505070309
```

Step 6 Save the file.

Step 7 Importing the modified file by selecting **import certificate specifications** under file menu of Entrust/admin.

Step 8 Verify the new certificate specifications by creating a user:

a Select **Add New User** under Users menu

b Enter the user information for the corresponding dialog box.

c Select **web** for ‘category’ and **valicert** for ‘type’ under the General Information tab.

d Click **apply**.

Step 9 Save the reference number under the Setup information tab.

Step 10 Once the entry is created for the OCSP responder, you may generate a VA OCSP request:

NOTE: It is important to use the **reference number** as the common name of the OCSP request.

Step 11 Launch Entrust WebConnector, and click on the Web Site Administrators menu.

Step 12 Select the “retrieve a site certificate for your Web server”.

Step 13 Input the reference number and authority code from the corresponding OCSP entry.

Step 14 Cut and paste the PKCS10 request into the text box.

Retrieving a Delegated Certificate

When you create a key pair for your ValiCert Enterprise VA, Enterprise VA generates a certificate signing request. Submit the certificate signing request to a CA to obtain a signed certificate from the CA.

For a local CA, the method you use to obtain a signed certificate, depends on the certificate server you use. Examples for using the following certificate servers are provided:

- Netscape CMS Server 4.1
- Microsoft Certificate Server

However, you can use a different certificate server.

NOTE: Your CA must be configured to issue certificates that include the fields specified in Table 6, “Extension Fields for Delegated Certificates,” on page 126.

If you are using the Netscape CMS Server 4.1, see below.

If you are using the Microsoft Certificate Server, skip to “Requesting a Certificate from a Microsoft Certificate Server 1.1” on page 136.

Requesting a Certificate from a Netscape CMS Server 4.1

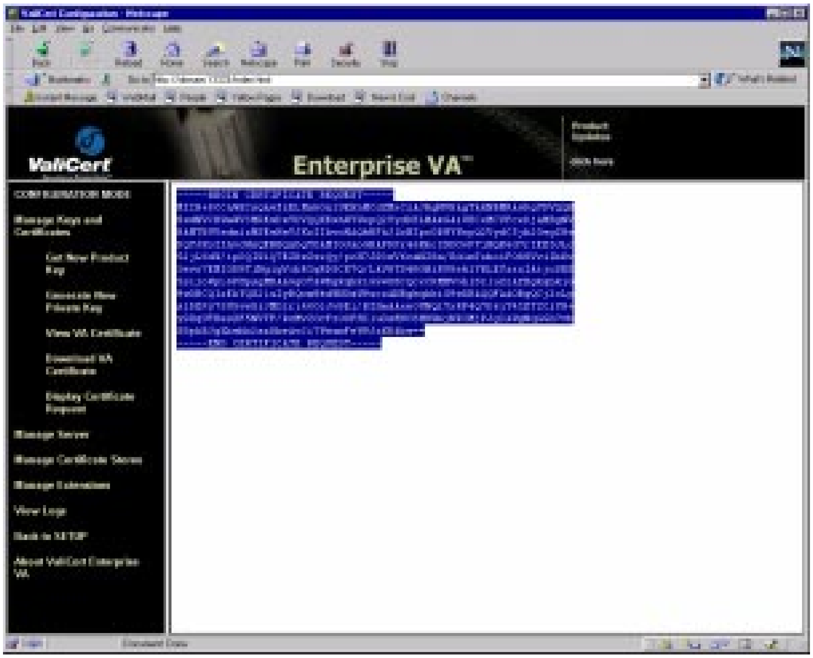
Use the steps in this section if you are using the Netscape CMS Server 4.1.

To submit a certificate signing request

Step 1 Click the **Display Certificate Request** item in the Enterprise VA Configuration Mode menu.

Step 2 Select the type of request and click **Display Certificate Request**.

A web page containing the certificate request displays:

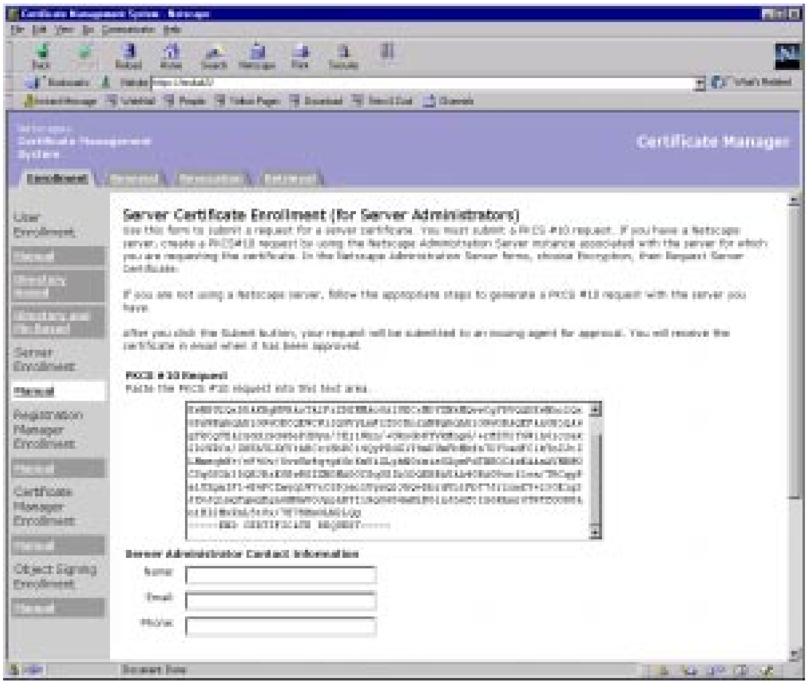


Step 3 Copy all the text to the clipboard. Include the lines containing **BEGIN CERTIFICATE REQUEST** and **END CERTIFICATE REQUEST**.

Step 4 Open the main Netscape CMS Server 4.1 web page in your browser.

Step 5 On the left-hand side of the screen under Server Enrollment, click Manual.

Step 6 The Server Certificate Enrollment (for Server Administrators) web page displays:



Server Certificate Enrollment (for Server Administrators)

Use this form to submit a request for a server certificate. You must submit a PKCS #10 request. If you have a Netscape server, create a PKCS#10 request by using the Netscape Administration Server instance associated with the server for which you are requesting the certificate. In the Netscape Administration Server forms, choose Encryption, then Request Server Certificate.

If you are not using a Netscape server, follow the appropriate steps to generate a PKCS #10 request with the server you have.

After you click the Submit button, your request will be submitted to an issuing agent for approval. You will receive the certificate in email when it has been approved.

PKCS #10 Request

Paste the PKCS #10 request into this text area.

```
[illegible]
-----END CERTIFICATE REQUEST-----
```

Server Administrator Contact Information

Name:

Email:

Phone:

Step 7 Paste the contents of the clipboard into the text area on this page.

Step 8 Enter your name, e-mail address, and phone number in the appropriate text fields.

Step 9 Click **Submit Request** at the bottom of the page.

The Request Successfully Submitted web page displays.

Step 10 Save this web page until you receive your signed certificate from the certificate authority.

Requesting a Certificate from a Microsoft Certificate Server 1.1

Use the steps in this section if you are using the Microsoft Certificate Server 1.1.

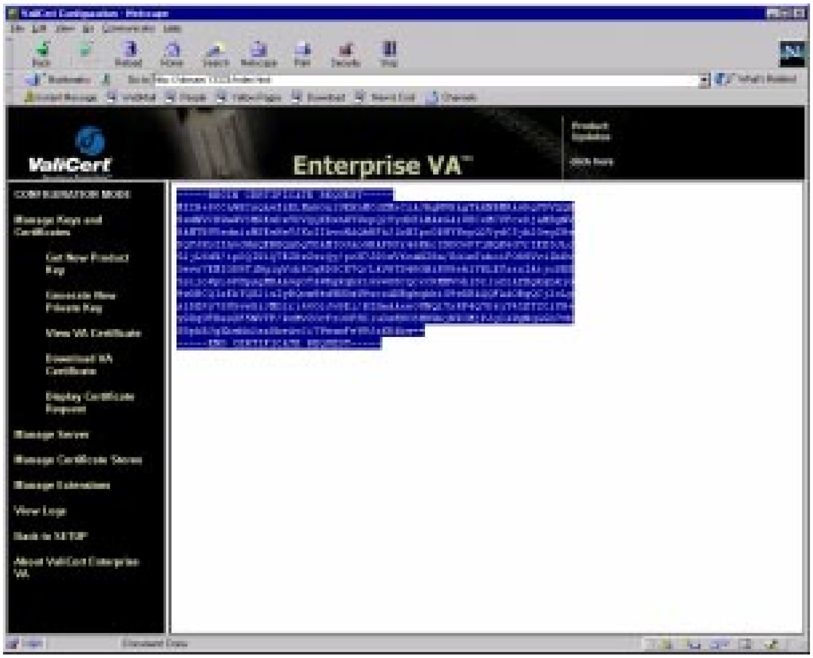
NOTE: If you are obtaining a root certificate from a Microsoft Certificate Server 1.1, you will need to use Internet Explorer 5.01 or newer as your web browser.

To create a certificate signing request

Step 1 Click the **Display Certificate Request** item in the Enterprise VA Configuration Mode menu.

Step 2 Select the type of request and click **Display Certificate Request**.

A web page containing the certificate request displays:



Step 3 Copy the entire certificate signing request to the clipboard.

Include the lines containing **BEGIN CERTIFICATE REQUEST** and **END CERTIFICATE REQUEST**.

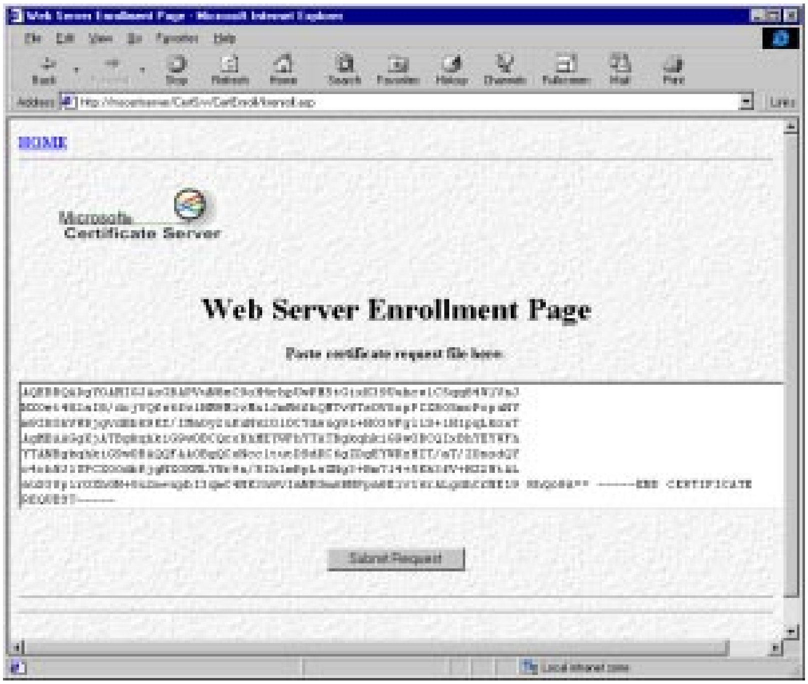
Step 4 Open the main Microsoft Certificate Server page in your browser.

Step 5 Click **Certificate Enrollment Tools**.

The Certificate Enrollment Tools page displays.

Step 6 Click the **Process a Certificate Request** link.

The Web Server Enrollment Page displays:


Web Server Enrollment Page - Microsoft Internet Explorer
File Edit View Go Favorites Help
Back Forward Stop Refresh Home Search Favorites History Channels Fullscreen Mail Print
Address
Links
HOME
Microsoft Certificate Server
Submit Request
Local intranet zone

Web Server Enrollment Page

Paste certificate request file here:

```
[illegible]
-----END CERTIFICATE
REQUEST-----
```

Step 7 Paste the certificate request that you copied into the Clipboard **Paste certificate request file here** area on this page.

Step 8 Click the **Submit Request** button at the bottom of the page.

Adding the Delegated Certificate

After you obtain the delegated certificate from the CA, add it to the certificate store so it can be used by your server to sign CRT and OCSP responses.

NOTE: Delegated certificates must contain the extensions specified in Table 6, “Extension Fields for Delegated Certificates,” on page 126.

For instructions on adding certificates, see “Adding the CA Root Certificate” on page 58.

APPENDIX B

Security Recommendations

This section contains security recommendations for sites that are running the Enterprise VA. The recommendations are categorized as follows:

- General
- Enterprise VA Administration Server
- Enterprise VA Host

NOTE: The default license is designed to enable 40-bit encryption. If you want a 128-bit encryption license and qualify under U.S. ITAR regulations, contact support@valicert.com for more information.

General

- Run Enterprise VA on a separate machine with no other software installed other than the operating system.
- Create only essential accounts on that machine (unauthorized users should not be allowed to log onto the machine).
- Locate the Enterprise VA machine in a physically secure location.
- Install vendor recommended patches - monitor the CERT and vendor lists to hear of new OS patches.
- Run on a machine with a good clock - set the time source once (potentially using NTP). Now disconnect the time source so that people cannot attack it. Make sure your time does not drift more than a few seconds a year. Check the time skew once a month.

Enterprise VA Administration Server

The Enterprise VA Administration Server can now be completely controlled remotely. Ensure that only authorized people can access this server. You can take various security measures to prevent unauthorized access. The following are measures listed in increasing order of security:

- Require a username/password to access Enterprise VA Administration Server.
- Require a username/password over an SSL session.
- Use SSL with client authentication.
- Use SSL with client auth and allow access to the Enterprise VA Administration Server port only from a select set of hosts.
- Shut down the Administration Server when not in use. Restart it only when needed. This follows the rule saying you want to run as little software on a secure machine as possible.

Enterprise VA Host

- Use the `maxMsgLen` variable in the `valicert.ini` file to limit the maximum message size anyone can send Enterprise VA.
- On NT, disable the domain login.
- On NT, run on an NTFS file system.
- Use a good password to protect your private key(s). Good passwords should contain letters in both cases and at least one digit and one punctuation and be at least 8 characters in length. They should not be dictionary words or personal words (your name, last name, name of somebody in your family/friend, names spelled backwards, /l replaced by 1, o replaced with 0).
- Monitor the Enterprise VA log for warnings.
- Disable ~stats/GET requests on Enterprise VA; set `enableGET` to 0 in `valicert.ini` file.
- Store the private key(s) on hardware. Administer the hardware well.
- Write your own product name as the value of the `Product` variable in the `valicert.ini` file.

CHAPTER
C

Security for VA Administration

This section describes how to set up an SSL session to allow your browser to communicate with the Enterprise VA Administration Server over a secure connection. This means that your browser will communicate with the Enterprise VA Administration Server over https instead of http. To setup a secure session, you must configure the apache-SSL server.

NOTE: The Administration Server is an apache server. If it is running in secure mode, it is also called the apache-SSL server.

The following procedures are described:

- ❖ Setting up SSL on Windows NT
- ❖ Setting Up SSL on UNIX

Setting up SSL on Windows NT

To set up an SSL session on Windows NT

Step 1 Set up the private key for the Administration Server (this is part of the Enterprise VA setup).

Step 2 Generate the private key file for the apache-ssl server and save it to a local file.

Step 3 Get the certificate of the CA that issued the server certificate and save to a local file. [optional]

Step 4 Open the `httpd.conf` file in the `apache\conf` folder.

Step 5 Enable loading of the SSL modules.

Remove the pound sign (#) at the beginning the following lines in the top section of the `httpd.conf` file to enable the SSL modules:

```
LoadModule ssl_module modules/ApacheModuleSSL.dll
LoadModule digest_module modules/ApacheModuleDigest.dll
```

Step 6 Enable other variables in the configuration file.

Remove the pound sign (#) at the beginning the following entries in the top section of the `httpd.conf` file:

```
SSLLog logs/ssl.log
SSLLogLevel none
SSLProtocol all
SSLVerifyClient none
SSLEngine off
```

Step 7 Set the SSL Engine variable to ON to configure the Administration Server in SSL mode:

```
SSLEngine on
```

NOTE: You can turn off SSL mode by changing the SSLEngine variable to off.

Step 8 Enable the SSLPassPhraseDialog entry.

This entry points to the path of the password dialog box executable. Remove the pound sign (#) at the beginning of the `SSLPassPhraseDialog entry`.

NOTE: Apache servers only recognize DOS style paths.Use an entry similar to the following:

```
SSLPassPhraseDialog exec:C:\PROGRA~1\ValiCert\EnterpriseVA/
Apache/password.exe
```

Do not use an entry similar to the following:

```
SSLPassPhraseDialog exec:C:\Program Files ValiCert\
EnterpriseVA/Apache/password.exe
```

Step 9 Enable the SSLCertificateFile variable and point it to the path of the SSL server certificate.

Remove the pound sign (#) at the beginning the entry.The following is an example:

```
SSLCertificateFile C:\PROGRA~1\VALICERT\EnterpriseVA\
entserv\ssladmin.cer
```

Step 10 Enable the SSLCertificateKeyFile variable and point it to the private key of the SSL server certificate.

Remove the pound sign (#) at the beginning the entry.The following is an example:

```
C:\PROGRA~1\VALICERT\EnterpriseVA\entserv\ssladmin.privkey
```

Step 11 (Optional.) Enable the SSLCertificateChainFile variable and point it to the CA certificate file.

Remove the pound sign (#) at the beginning the entry.The following is an example:

```
SSLCertificateChainFile C:\PROGRA~1\VALICERT\
EnterpriseVA\ entserv\ssladminca.cer
```

Setting Up SSL on UNIX

To set up an SSL session on UNIX

Step 1 Set up the private key for the Administration Server.

a Generate the private key file for the apache-ssl server and save it to a local file.

The following is an example of the full path of a local file:

```
/usr/local/valicert/va/apache/conf/
 ssladmin.privkey
```

b Specify the private key file’s absolute or relative path from ServerRoot in the `SSLCertificateKeyFile` variable.

The SSLCertificateKeyFile variable is defined in the `apache/conf/httpd.conf` file of your Enterprise VA installation. The following is an example of the in the SSLCertificateKeyFile variable setting in the `httpd.conf` file:

```
SSLCertificateKeyFile conf/ssladmin.privkey
```

Step 2 Set up the certificate for the Administration Server.

a Get the apache-ssl server certificate and save to a local file.

The following is an example of the full path of a local file:

```
/usr/local/valicert/enterpriseva/apache/conf/ssladmin.
cer
```

b Specify the server certificate's absolute or relative path from 'ServerRoot' in the SSLCertificateFile variable.

The SSLCertificateFile variable is defined in the `apache/conf/httpd.conf` file of your Enterprise VA installation. The following is an example of the variable setting in the `httpd.conf` file:

```
SSLCertificateFile conf/ssladmin.cer
```

Step 3 Set up the certificate chain for the Administration Server.

a Specify a file containing the concatenation of PEM encoded CA certificates in the SSLCertificateChainFile variable.

This files forms the certificate chain for the server certificate. The following is an example of the variable setting in the `httpd.conf` file:

```
SSLCertificateChainFile conf/ssladminca.cer
```

NOTE: Alternatively, the referenced file can be the same as SSLCertificateFile when the CA certificates are directly appended to the server certificate for convenience.

Step 4 Enable SSL for this host by setting the SSLEngine variable to ON.

The SSLEngine variable is defined in the `httpd.conf` file of your Enterprise VA installation. The following is an example of the variable setting in the `httpd.conf` file:

```
SSLEngine on
```

NOTE: The variables in Steps 1 through 4 are defined in the following section of the `httpd.conf` configuration file:

```
<IfDefine SSL>
##
## SSL Virtual Host Context
##
<VirtualHost_default:8443>
.
.
.
</VirtualHost>
```

Step 5 Define the port number for SSL connections:

The default port number for SSL transaction is: 8443 and is specified in <VirtualHost _default_:8443>. Place the same port number at the top of the `httpd.conf` file as follows:

```
##  SSL Support
##
##  When we also provide SSL we have to listen to the
##  standard HTTP port and to the HTTPS port
##
<IfDefine SSL>
Listen 8443
</IfDefine>
```

To listen on 443 for HTTPS requests, specify the following entries in the `httpd.conf` file:

```
<IfDefine SSL>
Listen 443
</IfDefine>
.
.
.

  <VirtualHost _default_:443>
```

Step 6 Restart the Administration Server in SSL mode using the following commands:

```
apache/bin/apachectl stop
apache/bin/apachectl startssl
```

APPENDIX

D

Setting up Hardware Acceleration Feature

This section provides information about setting up the hardware acceleration feature of which the most prominent part is hardware acceleration of signing functions (hardware signing). Hardware acceleration (HA) provides increased performance and greater key security. With hardware acceleration signing rates of over 100 requests per second can be achieved.

The hardware devices supported by Enterprise VA include:

- Chrysalis Luna 2, Luna CA, Luna CA3 and Luna XP
- nCipher nFast/CA (nShield) and nFast/KM (nForce)

NOTE: Chrysalis token firmware version 3.2 and later and PED firmware version 1.4 and later are required.

Both supported hardware types run under Windows NT and Solaris (UNIX).

Table 1 shows the libraries needed to communicate with leading hardware acceleration vendors.

Table 1. Release Library requirements

	NT	Solaris
Chrysalis (SCSI-based)	NA	7.0*
Chrysalis (PCI-based)	6.2	NA
nCipher (SCSI-based)	3.05	3.05
nCipher (PCI-based)	2.04	NA

* Chyrsalis is not supported on Solaris 2.5.1.

To use the hardware signing feature install and test the hardware. Then configure it to work with the Enterprise VA.

Installing Hardware Signing Devices

Install one of the approved PKCS11 devices on your host system following the manufacturer’s installation procedures.

Test the installation using the manufacturer's utilities. Confirm that the required libraries, drivers and servers are properly installed by verifying basic communication with the device (use `lunadiag` for Chrysalis and `enquiry` for nCipher).

NOTE: To simplify trouble shooting, confirm the Enterprise VA and hardware operation separately before integrating the two. First, use the hardware manufacturer’s utilities to confirm the hardware operation. Then use software signing to confirm Enterprise VA operation.

Configuring Hardware Signing Devices

To configure the devices, initialize and configure the token and generate the signing and encryption keys.

Initializing Tokens

The PKCS #11 specification defines a token as device that is capable of performing crypotgraphic operations. A token may be a physical device such as the Chrysalis Luna PCMIA card, or a logical device such as the smart card interface used by nCipher.

In either case the token must be initialized prior to use. Initialization is the process of formatting the hardware device with a user password and assigning it a token label.

The user password must be entered whenever Enterprise VA is invoked. The password must be issued to all personnel who may be called upon to start the Enterprise VA system.

Use a unique token label in order to avoid confusion in installations that use multiple tokens.

Initializing Chrysalis

A Security Officer password must also be created when initializing the token. The password should be different than the user password. The Security Officer password is used to change the user password and is not required for standard operation.

For added security, the Chrysalis Luna CA3 uses a Pin Entry Device (PED) that replaces a password with color coded keys. During initialization the device automatically generates PINs that are written directly to the physical keys. Prompts issued in the PED's LCD panel, guide you through this procedure.

Initializing nCipher

To enable token persistence, which allows the smart card to be removed once the accelerator has been initialized, specify this option when initializing the smart card with the "ckinitoken" utility.

Configuring Tokens

Tokens are complex devices that can be configured in various ways depending upon your operating environment. Some of the issues that should be considered when initializing a token include:

- Key cloning and backup
- M of N key support
- Token persistence (nCipher only)
- Device chaining (Chrysalis only)

Key Cloning

Key cloning allows the recovery of key data in the case of a lost or damaged hardware device. Follow the manufacturer’s recommendations regarding key backup to avoid having to issue new certificates in the case of token failure.

Configuring Chrysalis

In order to take advantage of scalable signing performance capabilities of the Chrysalis CA3/XP system, the optional load balancing extension library must be installed. Additionally key data must be cloned from the master CA3 device to the clone XP devices. This can be performed using the Chrysalis `enabler` utility that is included with the standard installation software.

Enter a dummy password when prompted and follow the directions displayed on the PED's display to do the actual login.

Configuring nCipher

Because key data for the nFast system is stored in encrypted format on the host system hard drive, it is important that the key repository data be backed up in addition to cloning the smart card which contains the key that is used to encrypt the signing keys.

Token persistence allows the smart card to be removed once the accelerator has been initialized. This option must be specified when initializing the smart card with the `ckinitoken` utility.

Generating Hardware Keys

Once you confirm the proper operation of the PKCS11 device, use it to generate signing and encryption keys through the Enterprise VA administrative interface. These keys operate in the same manner as software generated keys with the exception that the private key is stored either on the device (Chrysalis) or in an opaque key repository (nCipher).

NOTE: Enterprise VA does not support a mixture of hardware and software signing mechanisms.To use hardware signing you must generate hardware keys for all the functions that are applicable to your configuration.

Depending upon your server configuration, generate the following keys:

- ❖ OCSP response signing (required)
- ❖ SSL encryption key (required for SSL (https) operations)

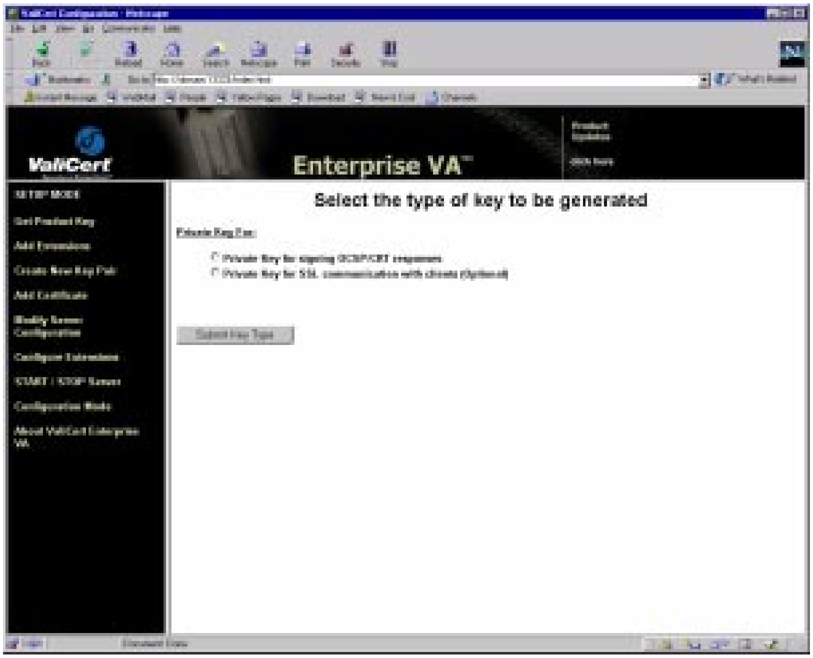
To create a new hardware key pair

Step 1 If necessary, to display the key pair page, from the Setup menu, click **Create New Key Pair**.

OR

From the Configuration Mode menu, under Manage Keys and Certificates, click **Generate New Private Key**.

The key pair web page displays:



Select the type of key to be generated

Private Key For:

○ Private Key for signing OCSP/CRT responses

○ Private Key for SSL communication with clients (Optional)

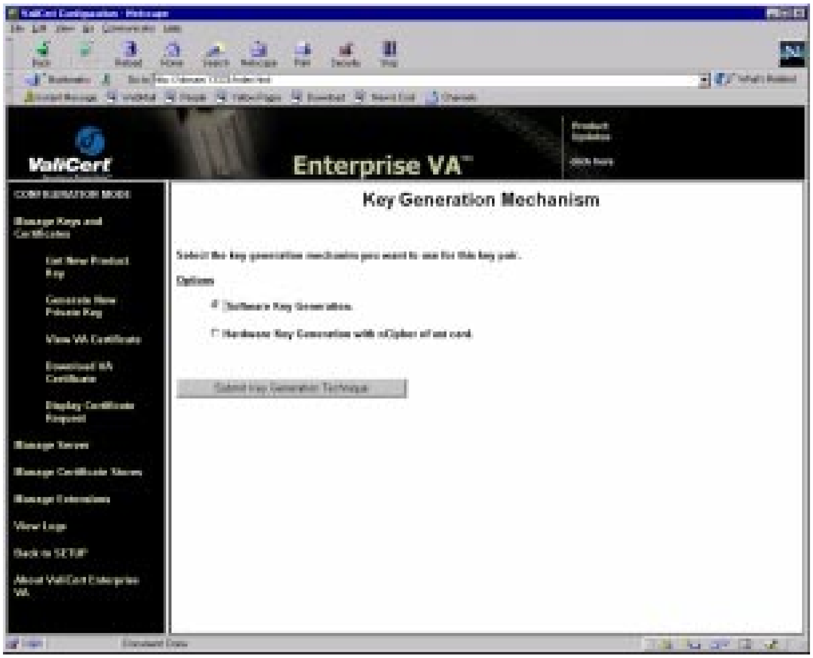
NOTE: If you have added extensions, more options may be available.

Step 2 Select a key type and click **Submit Key Type**.

NOTE: The Private Key for signing OCSP/CRT responses is required by the Enterprise VA.

The Private Key for SSL communication with clients is optional but is required for SSL communication.

The key generation mechanism page displays:



Key Generation Mechanism

Select the key generation mechanism you want to use for this key pair.

Options

● Software Key Generation.

○ Hardware Key Generation with nCipher nFast card.

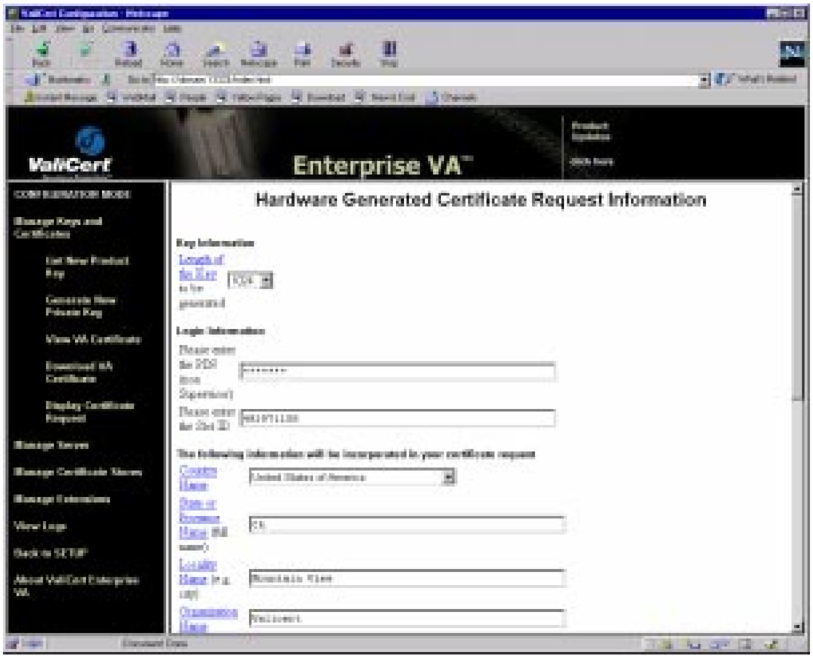
Submit Key Generation Technique

NOTE: If you do not have the hardware connected to your server this page will not display.

Step 3 To use hardware signing, select the Hardware Key Generation option.

Click **Submit Key Generation Technique**.

The Hardware Generated Certificate Request Information page appears:



Hardware Generated Certificate Request Information

Key Information

Length of the Key to be generated: 1024

Login Information

Please enter the PIN (from Supervisor): ********

Please enter the Slot ID: 492971558

The following information will be incorporated in your certificate request

Country Name: United States of America

State or Province Name (full name): CA

Locality Name (e.g. city): Mountain View

Organization Name: ValiCert

Step 4 The key pair is generated at the same time as a certificate request.

Enter the certificate request information.

Select the length of the Key to be generated from the **Key Information** list box. A key length of 1024 bytes should be sufficient for most applications.

NOTE: A key length of 2048 bytes may cause a timeout due to the amount of time necessary.

PIN: Enter the user PIN for your encryption hardware.

Slot ID: The first time you generate a key, this field contains the ID of the first active token. To use a different token, enter an alternate ID.

NOTE: For Chrysalis the token value will probably be 1. For nCipher this will be a multi-digit value like 492971558.

Country Name: Select the name of the country in which the server resides.

State or Province Name: Type the full name of the state or province in which the server resides.

Locality Name: Type the full name of the city in which the server resides.

Organization Name: Type the full name of the organization that “owns” the server, for example, Acme Corporation.

Organizational Unit Name: Type the full name of the unit within the organization that “owns” the server, for example, “Electronic Commerce Division.”

Common Name: Type the URL of the server, for example VES

E-Mail Address: Type the e-mail address of the server’s administrator.

Challenge Password: Type a password that you will use when retrieving the signed certificate. This password must be at least four characters long.

Alternative Company Name: Type the company name, without using any spaces between characters. (This is an optional field.)

Sign/Verification of data: This box must be checked for all keys.

Encryption/Decryption of data: This box must be checked when generating an SSL key since SSL performs encryption.

Wrap/Unwrap: This feature is currently not used.

Generate self-signed certificate: Select this option to generate a self-signed certificate.

The ValiCert Enterprise VA uses its self-signed certificate to sign validation responses. In this model, the client application needs to have both the CA root certificate and the ValiCert Enterprise VA root certificate in order to read the responses.

Do not generate self-signed certificate: Select this option to only generate a certificate request.

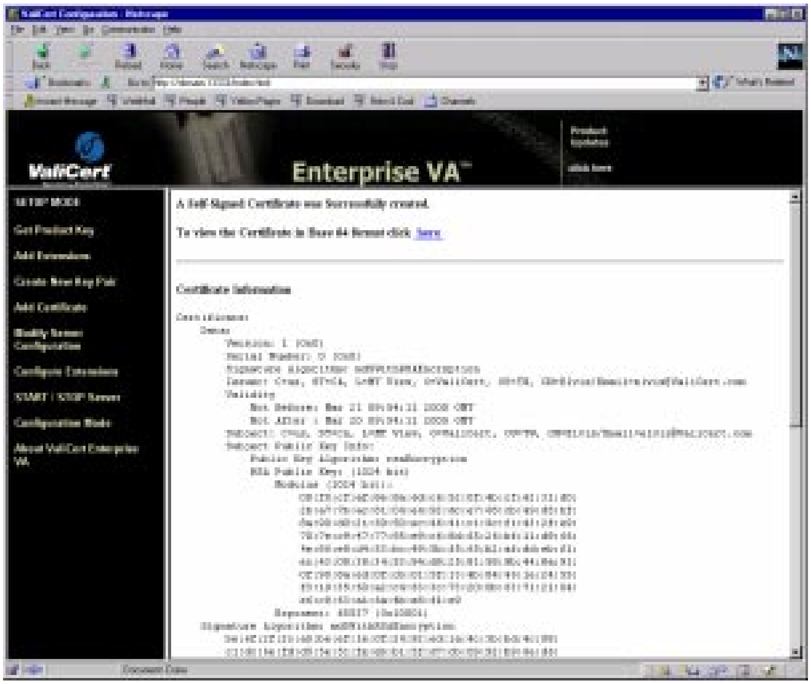
You must install the certificate you get from the CA after you submit the request. In this model, the ValiCert Enterprise VA uses a certificate signed by a CA to sign validation responses. This indicates that the ValiCert Enterprise VA is trusted by the CA to validate certificates. In this case, the client application only needs the CA root certificate in order to trust the responses.

NOTE: If you will be using a certificate signed by a CA, proceed to Appendix A, "Using Delegated Certificates." Do this prior to completing the remaining configuration tasks.

Step 5 Click **Submit Hardware Certificate Request**.

NOTE: This certificate is stored as `default.cert` in your `entserv` directory.

A web page containing the self-signed certificate information appears:



A Self Signed Certificate was Successfully created.

To view the Certificate in Base 64 format click here.

Certificate Information

```
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number: 0 (0x0)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: [illegible]
        Validity
            Not Before: Mar 21 09:34:11 2000 GMT
            Not After : Mar 20 09:34:11 2000 GMT
        Subject: [illegible]
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    [illegible]
                Exponent: 65537 (0x10001)
    Signature Algorithm: md5WithRSAEncryption
        [illegible]
```

Step 6 To proceed with the next step for first time configuration click **Next Step**. The next step is Adding the CA Root Certificate.

Server Startup

Once the hardware keys have been generated the server initialization file is automatically configured to use the accelerator and the new hardware keys.

When you invoke Enterprise VA configured for hardware acceleration the title of the password prompt dialog will be "PKCS11 Device PIN" (instead of "ValiCert Server Password" which is used otherwise). Enter the token user's PIN to start the Enterprise VA.

Assuming the password is correct, Enterprise VA verifies that the token private keys match the public key certificates. If they do not match a message will be written to the server log and the server will halt.

Assuming that the Enterprise VA starts properly, to test the signing keys use ValiCert's `ocspproof` utility. To check the SSL key access the server stats page, e.g. `https://<hostname>:<port>/~stats`.

Log in Using the Chrysalis CA3

For added security the CA3 replaces traditional password (PIN) entry with color coded data keys that were programmed during token initialization. Normal login is performed using the user (black) data key. The key must be entered and the "ENT" button must be depressed each time an application connects to the token (you are prompted via the LCD).

Because the Enterprise VA does not detect whether a CA3 device is in place Enterprise VA always prompts for a password. In this case enter a dummy password (any 4 digits) followed by the key entry procedure described above. This procedure must also be followed when creating signing keys through the administrative interface.

Starting with version 1.5.1 of the PED firmware it is no longer necessary to manually press the ENT button to complete the login process. If the appropriate data key is inserted in the device the login process will proceed automatically.

Trouble Shooting

In order to facilitate debugging, requests to PKCS#11 devices are logged to a log file which should be consulted if an operation fails. Key generation operations are logged to `evaAdmin.log` which is located in the

<INSTALL_DIR>/apache/cgi-bin. There is no Web interface to this file so it must be viewed manually. Enterprise VA status is logged to a dynamic log file that may be viewed via the administrative interface.

The following sections provide solutions to some common setup problems.

Could not load the specified PCKS11 library:

This error occurs when the vendor's PKSC#11 dynamic library could not be loaded. This indicates that the library could not be found or was invalid. The library path is obtained by looking in one of the following locations:

LibUnix in Crystoki2 section of /etc/Chrystoki.conf (Chrysalis/Solaris)

LibNt in Crystoki2 section of <OS_DIR>/Crystoki.ini (Chrysalis/NT)

*$NFAST_HOME/swspro/lib/libcknfast.so (nCipher/Solaris)

*$NFAST_HOME/bin/cknfast.dll (nCipher/NT)

*$NFAST_HOME defaults to /opt/nfast or c:/nfast if not set.

If the library fails to load check that the path exists.

Could not initialize the PKCS11 library:

This error indicates that the library could not establish contact with the PKCS#11 device driver. Check that the hardware is correctly connected and the requisite drivers and server (nCipher only) are running. In NT the device drivers can be reloaded by stopping and restarting them using the "Devices" dialog (under the "Control" panel). nFast devices also require that the nFast server is running.

Token in slot X is not responding:

Check that the token/smart card is firmly inserted into slot X. If the slot number is incorrect check the pkcs11SlotId value in the valicert.ini file.

No key file was written to the nCipher key repository:

The key generation process could not write the key data to the key database. This occurs if the key generation process does not have write access to the key repository. Check that the forms.exe group is nfast that the set group ID flag is set use the command:

```
ls -l forms.exe.
```

PKCS11 Activity Logging:

Difficult problems may be solved by enabling the PKCS#11 logging functions. Chrysalis devices use a "cklog" library that is interposed between the application and the PKCS#11 library. nCipher devices use a series of environment variables to control activity logging. See the appropriate vendor manuals for additional information regarding log configuration.

APPENDIX

E

Using the SNMP Agent

Enterprise VA includes a Simple Network Management Protocol (SNMP) agent to help you monitor the Enterprise VA through an SNMP Manager such as Hewlett Packard OpenView or Trivoli.

This section contains information in the following categories:

- Requirements for SNMP
- Installation instructions
- Configuration
- MIB definitions

This section describes the setup needed to use the SNMP agent with Enterprise VA on windows NT and Solaris.

Using SNMP with Windows NT

On NT, the SNMP agent runs as an extension to the native SNMP service. Make sure all the requirements are met, then install the Enterprise VA SNMP Agent on the same machine as the Enterprise VA host. To use the agent, load the MIBs at the SNMP manager.

Requirements for NT

- You must install the agent on the same host machine as the Enterprise VA.
- You must have administrator access to the host.
- You must have the SNMP Service installed.

NOTE: To get the SNMP service, install Options Pack 4 (or greater). Then add the SNMP service. For further instructions consult your Microsoft Documentation.

Installing the SNMP agent on Windows NT

To install the SNMP agent on NT, run the SNMP agent setup program. The program installs all the necessary components of the Agent.

To install the ValiCert Enterprise VA SNMP Agent on Windows NT

Step 1 Insert the CD containing the ValiCert Enterprise VA into your CD-ROM drive.

Step 2 Navigate to the SNMP folder.

Step 3 Double-click on the self-extracting file SNMPAgent32Setup.

Step 4 The Installation Folder dialog box displays.

Select a folder to extract the installation files into. If the folder does not exist you are prompted to create it.

Step 5 Click **Finish**.

Step 6 The installation files are unpacked and the Setup.exe program launches the Install Shield application.

The Welcome dialog box displays.

Follow the on-screen instructions as you proceed through the installation.

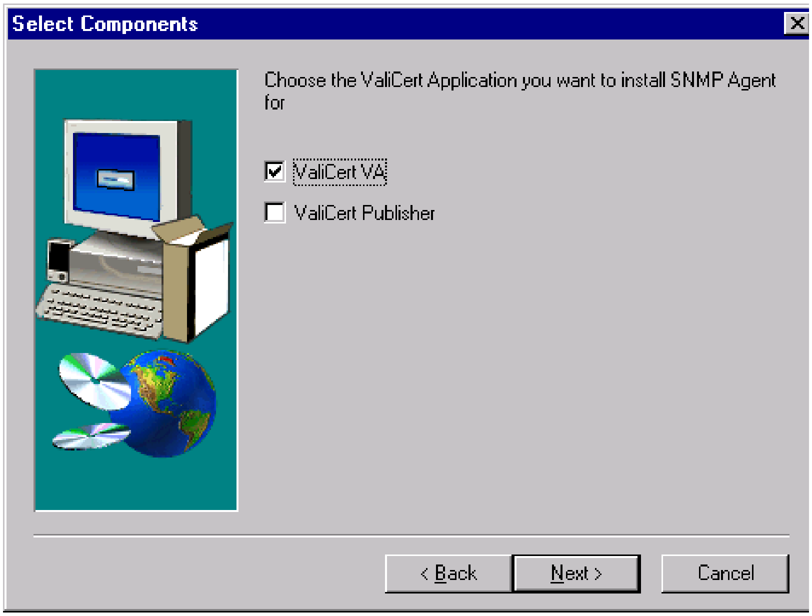
> The **Next** button allows you to move forward to the next installation window.
>
> The **Back** button allows you to return to the previous installation window
>
> The **Cancel** button closes the installation program without installing any component of the Enterprise VA SNMP Agent. To install Enterprise VA SNMP Agent, rerun the setup program.

Step 7 Click **Next**.

The ValiCert Software License Agreement dialog box displays.

Step 8 Click **Yes** to accept the license agreement.

The Select Components dialog box displays:



Select Components

Choose the ValiCert Application you want to install SNMP Agent for

☑ ValiCert VA

□ ValiCert Publisher

Step 9 Select the ValiCert VA checkbox.

Step 10 Click **Next**.

The Agent installs and the Setup Complete dialog box displays

Step 11 Select to display the README and if you want to start the SNMP agent.

Step 12 Click **Finish**.

Using SNMP with UNIX (Solaris)

On UNIX, the SNMP agent runs as a `.tcl` script called `evaAgent.tcl`. The Enterprise VA SNMP Agent is installed with the Enterprise VA host.

To use the agent, load the MIBs at the SNMP manager.

Requirements

- You must have administrator access to the host.
- You must have scotty (the TCl/TK Extension for SNMP) installed.

Installing Scotty

If you do not have scotty, install it from the CD. The file is called `scottr.tar`. To install it type:

```
tar -xvf scotty.tar
```

Running the SNMP Agent for UNIX

To start the agent, at the prompt type:

```
scotty evaAgent.tcl
```

Configuring the SNMP Agent

To configure the SNMP agent (for Windows NT or for UNIX (Solaris) you must manually edit the file `valicert.ini` which is installed in the `entserv` directory of the Enterprise VA installation. To do this open the file in a text editor and make the desired changes. Table 1 below specifies the SNMP variables and their default values.

Windows NT

Traps and the ports used are native to the OS so no configuration of these is necessary. To set the polling period and turn on or off the traps edit the variables in the `ini` file.

UNIX (Solaris)

To specify the required host and port information and to enable traps edit the variables in the `ini` file.

SNMP Variables

The following are the SNMP variables contained in the `valicert.ini` file.

Table 1. SNMP Variables

Variable	Definition	Default Value
`[snmp]`	The section name for the Simple Network Management Protocol configuration section.	
`pollafter`	The frequency (in seconds) that the agent updates the MIB variables.	`300`, Optional
`enableEvaTrap`	This determines whether the trap for the Enterprise VA server being down is on or not. Set to `0` for off, or `1` for on.	`0`, Optional
`enableEvaAdminTrap`	This determines whether the trap for the administration server being down is on or not. Set to `0` for off, or `1` for on.	`0`, Optional
`agentport`	The port to which the agent sends traps. This variable applies to UNIX (Solaris) only.	`10040`, Optional
`masterHost`	The hostname of the SNMP Manager. This variable applies to UNIX (Solaris) only.	`0`, Optional
`masterport`	The port on which the Manager listens for the agent. This variable applies to UNIX (Solaris) only.	`10040`, Optional

MIB Variables

The following are the MIB variables used by the SNMP agent for the Enterprise VA.

Regular

```
VAS-STATS-MIB DEFINITIONS ::= BEGIN
    IMPORTS
        enterprises     FROM RFC1155-SMI
        DisplayString   FROM RFC1213-MIB
        OBJECT-TYPE     FROM RFC-1212;

   valicert             OBJECT IDENTIFIER ::= {enterprises 2930}
   SNMP                  OBJECT IDENTIFIER ::= {valicert 5}
   server        OBJECT IDENTIFIER ::= {SNMP  2}
   EVA                   OBJECT IDENTIFIER ::= {server 1}
```

```
        stats      OBJECT IDENTIFIER ::= {EVA 1}
--
***************************************************************
*************

    MibRevMajor OBJECT-TYPE
        SYNTAX  INTEGER (1..65535)
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
            "The major revision level of the MIB.
        This value tracks major functional changes made to the
MIB."
        ::= { stats 1 }

    MibRevMinor OBJECT-TYPE
        SYNTAX  INTEGER (0..65535)
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
            "The minor revision level of the MIB.
        This value tracks minor changes made to the MIB."
        ::= { stats 2 }

    ServerVersion OBJECT-TYPE
   SYNTAX  DisplayString (SIZE (1..255))
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
            "VA server’s version string
        This string value indicates the VA’s version number."
        ::= { stats 3 }


    StartTime  OBJECT-TYPE
        SYNTAX  DisplayString (SIZE (1..255))
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
            "The time at which the server was started."
        ::= { stats 4 }

    InstanceOfServer OBJECT-TYPE
        SYNTAX  INTEGER (0..65535)
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
            "The number of server instances currently running."
        ::= { stats 5 }


    CrlsReceived OBJECT-TYPE
        SYNTAX INTEGER (0..65535)
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
            "The number of CRLs the VA received since it was
started."
        ::= { stats 6 }

    CasInGlobalCrt OBJECT-TYPE
        SYNTAX INTEGER (0..65535)
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
            "The number of CA certificates in the VA trusted
certificate store."
        ::= { stats 7 }


    LeavesInGlobalCrt OBJECT-TYPE
        SYNTAX INTEGER (0..65535)
   ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
            "Number of leaves in the CRT."
        ::= { stats 8}

    CasInLocalCrt OBJECT-TYPE
        SYNTAX INTEGER (0..65535)
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
            "The number of CA certificates in the VA trusted
certificate store."
        ::= { stats 9 }


    LeavesInLocalCrt OBJECT-TYPE
        SYNTAX INTEGER (0..65535)
   ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
            "Number of leaves in the CRT."
        ::= { stats 10}


    OkCertsCheckedWithCrt OBJECT-TYPE
        SYNTAX INTEGER (0..65535)
   ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
            "The number of valid certificates checked using the
CRT protocol."
        ::= { stats 11 }

    RevokedCertsCheckedWithCrt OBJECT-TYPE
        SYNTAX INTEGER (0..65535)
   ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
           "The number of revoked certificates checked using the
CRT protocol."
        ::= { stats 12 }

    UnknowCaCheckedWithCrt OBJECT-TYPE
        SYNTAX INTEGER (0..65535)
   ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
            "The number of certificates issued by an untrusted
CA, which have been checked using the CRT protocol."
        ::= { stats 13 }

    ErrorCertsCheckedWithCrt OBJECT-TYPE
        SYNTAX INTEGER (0..65535)
   ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
            "The number of erroneous certificates checked using
the CRT protocol."
        ::= { stats 14 }

    OkCertsCheckedWithOcsp OBJECT-TYPE
        SYNTAX INTEGER (0..65535)
   ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
```

```
           "The number of valid certificates checked using the
OCSP protocol."
        ::= { stats 15 }

    RevokedCertsCheckedWithOcsp OBJECT-TYPE
        SYNTAX INTEGER (0..65535)
   ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
          "The number of revoked certificates checked using the
OCSP protocol."
        ::= { stats 16 }

    UnknowCaCheckedWithOcsp OBJECT-TYPE
        SYNTAX INTEGER (0..65535)
   ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
            "The number of certificates issued by an untrusted
CA, which have been checked using OCSP."
        ::= { stats 17 }

    ErrorCertsCheckedWithOcsp OBJECT-TYPE
        SYNTAX INTEGER (0..65535)
   ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
           "The number of erroneous certificates checked using
OCSP."
        ::= { stats 18 }

    NumberOfCrtRequests  OBJECT-TYPE
        SYNTAX INTEGER (0..65535)
   ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
            "The number of CRT requests the VA has served."
        ::= { stats 19}

    NumberOfOcspRequests  OBJECT-TYPE
        SYNTAX INTEGER (0..65535)
   ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
            "The number of OCSP requests the VA has served."
        ::= { stats 20}
    MemoryUsed  OBJECT-TYPE
        SYNTAX INTEGER
   ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
            "The amount of system memory the VA process is
currently using."
        ::= { stats 21}


    LastErrorMsg OBJECT-TYPE
   SYNTAX  DisplayString (SIZE (1..2048))
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
            "The latest ERROR message from the VA server"
        ::= { stats 22 }

    LastWarningMsg OBJECT-TYPE
   SYNTAX  DisplayString (SIZE (1..2048))
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
            "The latest WARNING message from the VA server"
        ::= { stats 23 }

    LastAdminAction OBJECT-TYPE
   SYNTAX  DisplayString (SIZE (1..2048))
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
        "The latest administrative task performed on the VA."
        ::= { stats 24 }


    LastAdminWarning OBJECT-TYPE
   SYNTAX  DisplayString (SIZE (1..2048))
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
            "Latest WARNING message from VA Admin."
        ::= { stats 25 }

    LastAdminError OBJECT-TYPE
   SYNTAX  DisplayString (SIZE (1..2048))
```

```
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
            "Latest ERROR message from VA Admin."
        ::= { stats 26 }

-- we can add as many variable as we need

END
```

Traps

```
EVA-TRAPS-MIB DEFINITIONS ::= BEGIN
    IMPORTS
        enterprises     FROM RFC1155-SMI
   DisplayString   FROM RFC1213-MIB
   OBJECT-TYPE     FROM RFC-1212
        TRAP-TYPE       FROM RFC-1215;

   valicert             OBJECT IDENTIFIER ::= {enterprises 2930}
   SNMP                  OBJECT IDENTIFIER ::= {valicert 5}
   server        OBJECT IDENTIFIER ::= {SNMP  2}
   EVA                   OBJECT IDENTIFIER ::= {server 1}
   traps                 OBJECT IDENTIFIER ::= {EVA 2}
--
***************************************************************
*************

    Major           OBJECT-TYPE
                    SYNTAX  INTEGER (1..65535)
                    ACCESS  read-only
                    STATUS  mandatory
                    DESCRIPTION
                    "The major revision of the MIB

                    Major."
                    ::= { traps 1 }

    Minor           OBJECT-TYPE
                    SYNTAX  INTEGER (0..65535)
                    ACCESS  read-only
                    STATUS  mandatory
                    DESCRIPTION
                    "The minor revision of the MIB  Minor"
                    ::= { traps 2 }

-- Traps
```

```
        ServerIsDown                TRAP-TYPE
                                    ENTERPRISE  traps
                                    DESCRIPTION
                                    "EVA Server is down."
                                    ::=  50

        AdminServerDown             TRAP-TYPE
                                    ENTERPRISE  traps
                                    DESCRIPTION
                                    "EVA Admin Server is down."
                                    ::=  51

    END
```

APPENDIX

F

Troubleshooting

This section contains troubleshooting information in the following categories:

- Installation troubleshooting
- Configuration troubleshooting
- Usage Troubleshooting
- Error Messages

Installation Troubleshooting

Problem: You see an Apache error message

Solutions:

The port you have selected for the Apache (Administration) server is already in use.

DNS is not configured in the machine’s TCP/IP properties (Windows NT).

Problem: Installation fails

Solutions:

You are not logged into the machine either as its Administrator, or as a member of the Administrators group.

Your disk is full.

You are running an old Service Pack (Windows NT); make sure you are using either SP3 or SP5, but not SP4.

Problem: Installation of Apache fails and a "Service Not Started" message displays when use attempts to connect to the Administration Server.

This may indicate that Apache has not been installed correctly.

Solutions: If Apache can not resolve its hostname, the Apache service does not install.

Problem: An error message displays "Can't determine EVA/CVA version" and the Installer quits.

Solutions: This happens if there is more than one registry entry for Enterprise VA. (For example you are upgrading and there is an entry for versions 3.0 and 3.2). Delete one of the registry entries and reinstall (re-upgrade).

Configuration Troubleshooting

Problem: I can’t create a new key pair.

Solutions:

Your browser is not working with the Javascript key generator; you must use a newer browser. ValiCert recommends Microsoft IE5 or Netscape Communicator 4.5 or later.

If you are using an SSL connection, be sure that you use Netscape Communicator 4.61 or above as your browser. Known incompatibilities exist when generating a key pair using Microsoft Internet Explorer.

Problem: I can’t configure the other ValiCert components (VA Publisher and Validators) from the Enterprise VA Administration Server.

Solutions:

You do not have Microsoft Internet Explorer 4.01 or above running on the machine you have installed the Enterprise VA. Install Microsoft Internet Explorer 4.01 or above and try to configure the other ValiCert components again.

Usage Troubleshooting

Problem: Enterprise VA won’t start, either at machine boot or via manual control.

Solutions:

You have not installed an active license file; see `http://localhost:13333` (port number of Administration Console) and follow directions

Your evaluation license has expired; request another one via the Administration Console

A port usage conflict has developed; verify that no other services are using either your Enterprise VA or Administration ports.

Your machine's IP address has changed; either change it back or request a new license for the `HostID` reported in the Administration Console.

You entered the incorrect password to unlock the Enterprise VA's private key; restart the Enterprise VA and enter the correct password.

Problem: When loading the Administration Console, I receive an HTTP error and the upper-right frame doesn't display correctly

Solution: That frame is populated by content served from ValiCert's corporate web server; if your machine is behind a firewall or otherwise unable to access the internet, this frame will not be populated and you will receive the HTTP error message.

Problem: I'm not sure if my Enterprise VA is active; how do I check?

Solution: Point your web browser to `http://machinename:Evaport`; if you see a ValiCert text response, your Enterprise VA is running.

Problem: I need to know a summary of my Enterprise VA's activity since it was last restarted; how do I get one?

Solution: Point your web browser to http://machinename:Evaport/~stats; you should see a table summarizing your Enterprise VA's activity.

Problem: The Administration Console doesn't look right.

Solution: Use a newer browser; the Console uses frames and Javascript. ValiCert recommends Microsoft IE5 or Netscape Communicator 4.5.

Problem: The Enterprise VA treats a CRL as expired when it is not expired.

Solution: Be sure that your CA and VA clocks are synchronized.

Problem: The Enterprise VA is down and there is a bind 125 error in the log file.

Solution: A bind 125 error means that another process is listening on the same port as the Enterprise VA, (either the server host port or the ssl server host port).

To fix this problem either change the ports that the Enterprise VA is using (through the administration GUI) or stop the other process that is conflicting with the Enterprise VA.

Error Messages

This section describes error messages the Enterprise VA places in log files that you can view. Each description includes the cause of the error and the action to take, if one is required.

For information about how to view these logs, see “Viewing Logs” on page 91.

ISCRT_ERR_CERTFORMAT

The Global VA Service root certificate is not in the correct format. Check the variable vgvsCertFile in `valicert.ini` and make sure it points to the Global VA Service root certificate.

ISCRT_ERR_CRLVERIFY: ISCRT_ERR_CRL_FROM_UNTRUSTED_CA

This error can occur when publishing CRL's to the Enterprise VA, if the CA's certificate is not trusted.

This error can also be reported by an Enterprise VA caching data from a Global VA Service. In this case check the vgvsCertFile variable in the `valicert.ini` file and make sure it points to the Global VA Service root. The error indicates that the Enterprise VA is not able to verify the signature on the Tree header it received from the Global VA Service.

This error can occur if the name on the CRL does not match the list of CAs trusted by the Enterprise VA. In case you are using different certificates for CA certificate signing and CRL signing make sure you trust both the CA roots.

This error can occur if the private key used to sign the CRL does not match t the public key in the certificate which is used to verify the CRL.

ISCRT_ERR_MEMORY

Out of memory. Close some applications.

ISCRT_ERR_FORMAT

The OCSP/CRT query is not properly constructed or there is an error in the transmission of the CRL from the publisher to the Enterprise VA. Make sure the publisher is able to retrieve the CRL correctly from its sources. Use the CRL_FILE_IN variable in the `vpublish.ini` file to verify that the CRL is received correctly.

The CRL could be malformed.

ISCRT_ERR_READ

Reported in communication with OCSP/CRT clients to Enterprise VA/Global VA Service or Enterprise VA/Global VA Service caching. Possible causes are as follows:

- Socket read error
- Lost connection to client.
- Very slow connection.

ISCRT_ERR_INVALIDARGUMENT

- Invalid port number specified in the valicert.ini for variable masterHosts.
- Invalid algorithm specified to the Enterprise VA for creating signatures.
- The root hashes did not match for the Enterprise VA/Global VA Service caching. The public/private key pair do not match for the Global VA Service.

ISCRT_ERR_OPEN/ISCRT_ERR_WRITE

- Cannot open file specified for reading/writing. Check for the existence of the file if it is meant to be read or check for permissions if specified for writing.
- Cannot create socket. Too many connections or out of memory.

ISCRT_ERR_VERSION

Version mismatch between the Enterprise VA/Global VA Service or CI/Global VA Service.

ISCRT_ERR_OLD_TREE

The CI or the Enterprise VA already has the tree which is sent by the Global VA Service. Check clock times and time zones to fix this.

ISCRT_ERR_OLD_INCREMENTAL_REQUEST

The Global VA Service does not have enough incremental data. The CI/Enterprise VA then requests for the full update of the data.

This can also occur when the Enterprise VA is down for a while and requests incremental data when it starts up.

ISCRT_ERR_PUBKEY

Badly formatted certificate or corrupted certificate.

ISCRT_ERR_MDTYPE

The specified MessageDigest is not found. The CRL is signed by some algorithms which are not supported by the Enterprise VA.

ISCRT_ERR_VERIFY

Error in signature verification of data. This is a lower-level error, typically logged with other errors.

ISCRT_ERR_SIGNFAILURE

RSA_private_encrypt bsafe function failed. Data is not correctly formatted for signing.

ISCRT_ERR_ALGO

Only RSA signing is supported for signing/verification. The certificate might be issued with a DSA key.

ISCRT_ERR_SIGNTOOBIG

Data returned by the RSA_private_encrypt function is more than what is expected of that signature (128 bytes).

ISCRT_ERR_NOAPPLICABLETREE

No tree found for a CRT request.

ISCRT_ERR_OLDCRL

The CRL is already with the Enterprise VA and the Enterprise VA has a newer CRL. The nextUpdate in the CRL has elapsed.

ISCRT_ERR_NOAUTHCERT

No certificate to issue CRT responses, or the certificate has a OCSP/CRT oid or an incorrect oid.

ISCRT_ERR_CRL_FROM_UNTRUSTED_CA

No certificate to issue CRT responses, or the certificate has a OCSP/CRT oid or an incorrect oid

ISCRT_ERR_NOOCSPSUPPORT

No signing certificate/private key configured for the Enterprise VA.

ISCRT_ERR_ALREADYHAVECRL

CRL already present.

ISCRT_ERR_UNKNOWNCRITICALEXTENSION

CRL-DPs are sent to the Enterprise VA, or any other critical extension is submitted.

ISCRT_ERR_NOTIMPLEMENTED

Received a CRT query, but the Enterprise VA was not configured to process CRTs.

Index